An Adaptive Security Framework for Evaluating and Assessing Security Implementations in PaaS Cloud Models

Olushola Alexander Akinbi

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS OF EDGE HILL UNIVERSITY, FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

September 2015

AUTHORS DECLARATION

This thesis is submitted to Edge Hill University in support of my application for the degree of Doctor of Philosophy. It has been composed by myself, all copyrighted material appearing in this thesis and all such use, has been clearly acknowledged. This thesis has not been submitted in any previous application for any degree.

ACKNOWLEDGEMENTS

I would like to express my unfeigned gratitude to my supervisor and mentor Professor Ella Pereira for her continuous support and encouragement throughout my PhD study. It has been an incredible journey I must say and I sincerely appreciate her support, knowledge, and expertise throughout the completion of this work. Her work ethic and professionalism have been exceptional and I owe my success to her guidance.

I also want to thank Dr. Chris Beaumont for his support and mentorship as part of my supervisory team. Your professionalism has really helped enhance my personal development within the last few years.

Sincere gratitude go to my PhD colleagues, Dan Campbell and Daniel Kay for making the PhD experience worthwhile. The times we shared in the labs and offices have made my experience enjoyable and full of fun.

A very special thank you to my darling wife Nneka. For your love, support, encouragement and understanding throughout the completion of this study. I love you! And finally to my adorable daughter Crissa, who was born during the time I was completing my thesis write up. You mean the world to me my princess.

ABSTRACT

The security risks of cloud computing and ambiguity of security mechanisms implemented on an on-demand cloud service such as Platform-as-a-Service (PaaS), continues to raise concerns by cloud consumers. These concerns continue to hinder the adoption of the potentials offered by provisioning of computer resources of this scale. It also indicates a lot needs to be done to improve security controls implemented on cloud computing services as a whole.

There is the need to understand and evaluate security mechanisms and controls implemented to preserve the confidentiality, integrity and availability of data stored, processed and accessed in the cloud. Also there is the need to ensure these mechanisms meet security standards and requirements to mitigate any security risks. Although most organisations and cloud service providers (CSPs) have various information security management systems they used to evaluate their computer security and CSPs try to obtain security certifications based on industry standards, cloud customers are however not sure of the security mechanisms implemented on cloud services and how these mechanism are integrated to provide adequate security for their data and applications developed and deployed in the cloud.

This research study highlights the use of a systematic and comprehensive approach developed by the researcher to understand in detail, the security architecture of PaaS clouds. This approach presents the development of a security framework which is used as a tool in an attempt to identify and evaluate security mechanism implemented on each PaaS component. The primary findings and preliminary analysis of the evaluation enabled the researcher determine the security provisions, capabilities and limitations of security features implemented on this type of cloud delivery model.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF PUBLICATIONS

Akinbi. A., Pereira. E. & Beaumont. C. "Identifying Security Methods and Controls for Secure PaaS Cloud Environments" 2013. 14th Annual PGnet Symposium.

Akinbi. A., Pereira. E. & Beaumont. C. "Evaluating Security Mechanisms Implemented on Public PaaS Cloud Environments: Windows Azure Case study. 2013. 8th International Conference for Internet Technology and Secure Transactions, ICITST.

Akinbi. A., & Pereira. E. "Mapping Security Requirements to Identify Critical Security Areas of Focus on PaaS Cloud Models". 15th IEEE International Conference on Computer and Information Technology, 2015.

Chapter 1 : INTRODUCTION

1.1 OVERVIEW

Computer security is defined as the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources [3][4]. Ensuring these objectives are met requires putting in place a security mechanism to detect, prevent computer systems from security attacks, or ensure speedy recovery in the event of such attacks [3].

In traditional information systems, the responsibility of ensuring these objectives are met is managed by IT administrators, security experts and users to ensure adequate security mechanisms are implemented, configured and deployed. However, in cloud computing, computer security responsibilities has shifted towards cloud service providers (CSPs) who offer computer resources as a service on a pay as you go basis; than cloud customers who subscribe to use the service. Therefore this leaves customers wondering what are the security mechanisms put in place by CSPs in cloud environments and how they can be certain their information resources will be secure if they choose to adopt cloud computing.

The Information Security Media Group [5] in a cloud security survey stated that, "CSPs hold greater responsibility for ensuring security of cloud resources followed by the organisation or customer adopting the cloud service. These responsibilities they concluded, involve implementing adequate security controls such as data encryption techniques, stronger ID/ access management controls and auditing of cloud service provisioning; a joint responsibility that should be shared by both

stakeholders". Every cloud service provider has provisioned various security measures depending on its cloud offering and architecture [6] and many security guidelines, standards and frameworks have been proposed by experts and researchers in the field towards security management and evaluation in the cloud. However, there is no one size fit all framework or security mechanisms able to accommodate both the dynamic nature of cloud architectures and shared management responsibilities between cloud providers and customers.

Cloud service providers offer three major service delivery models. Offered by top providers such as Salesforce, Google, Amazon, Microsoft, Sun Microsystems and IBM include Software-as-a-service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-service (IaaS). Other services such as Identity-as-a-Service (IDaaS) and Security-as-a-Service (SECaaS) are considered as additional service provisions that are embedded or integrated into the benefits of cloud computing adoption. The different models suggests different cloud architectures as well as different security implementations used to secure each model. Moreover, not all CSPs publicly share comprehensive information relating to their host platforms, security mechanisms to secure the hosts and host operating systems since hackers can exploit such information when trying to intrude into the cloud service [7]. However in recent years, there has been demand for transparency in the area of security implementations and provisions used to secure cloud computing resources and architectures. Security management standards such as the ITIL, CSA, NIST and ISO/IEC 27001 and 27002 to mention a few, set up by computer societies, are relevant as a set of best practices, guidelines and practices for managing security related to cloud computing technology.

These industry security guidelines, frameworks and standards revolve only around IT governance and customer relation management (CRM) established between CSPs and customers which are agreed

and documented in service level agreements (SLAs). The SLAs depend on the services rendered and service cost. The industry standards do not specify the required security mechanisms that should be put in place on service delivery models in the cloud but rather offer recommendations based on industry best practices in maintaining information security. Cloud customers are faced with the issues and challenges of selecting cloud services as well as evaluating security implementations on clouds based on their own security needs. Hence, there is the need for an approach to how this can be achieved and ensure security implementations and provisions are fit for purpose to meet not just industry guidelines; but customer security needs with respect to specific cloud models and their architecture. This will enable cloud customers, a clear understanding to demand adequate security as a service (SECaaS) which is offered through security provisions and features implemented in cloud models. It also will enable customers make the right choice of CSPs in relation to their security demands.

Services offered by CSPs vary from application development, software to infrastructure through cloud models. The security management also varies depending on several factors such as the deployment model and service level agreements. This study focuses on PaaS cloud models, as existing industry frameworks are focused on cloud computing security in general. On the other hand, related studies in this area have focused their attention on comparing security provisions offered by CSPs in various PaaS cloud environments with no consideration for methods evaluating how these security provisions meet certain security requirements. Moreover, methods of capturing security requirements that are specific for cloud service deployment and delivery models is considered very challenging in assessing security implementations in cloud environments especially for PaaS cloud models.

Evaluating security provisions and implementations in any cloud model requires an extensive security approach that ensures the identity and resources of entities and the cloud architecture are preserved. It also requires the security implementations used to preserve these resources are tested for possible vulnerabilities or threats; and meet security requirements and criteria established by the customer's service level objectives. According to CSA [8], "*The challenges with PaaS can be similar to SaaS, in addition to providing the necessary provisioning capabilities to the developers in the form of APIs. Currently, APIs that support identity provisioning on PaaS platforms are lacking*". Authenticating users in PaaS cloud environments guarantees the authorised users' credentials are valid. An appropriate mechanism need to be in place to ensure this is possible and protect users' credentials from possible security attacks at all times and if users have multiple passwords on PaaS accounts, how can they keep track of them in a secured manner?

Managing access control of authorised users by monitoring and auditing source codes used in developing web based applications in the cloud is essential in PaaS cloud security. Likewise, keeping track of authorised users from deliberately attacking the platform which supports multi-tenants from compromising other user's data in the cloud needs to be prevented or detected.

This research highlights the security risks of cloud computing and ambiguity of security mechanisms implemented on an on-demand cloud service like Platform-as-a-Service (PaaS), as it continues to raise concerns by cloud consumers in the adoption of the potentials offered by provisioning of computer resources of this scale. Examining on-demand Platform-as-a-Service public cloud environments, across various cloud service providers, this research thesis focuses on the security controls and mechanisms implemented on each of the PaaS cloud components. The research focuses on developing a security framework which consists of industry standard guidelines to evaluate the security offerings on PaaS clouds in an attempt to understand how its security controls and

implementations meet the needs of customers in providing confidentiality, integrity and availability in the development of web based applications hosted on the cloud. Hence providing an efficient security analysis of PaaS cloud models.

1.2 MOTIVATION

There is a critical need to systematically and comprehensively evaluate the security mechanisms implemented to meet security requirements to ensure computer security is failsafe and provided on PaaS cloud environments. For each security requirement there should be an evaluation to determine if there is a security solution available in the cloud marketplace or if the requirement should be met by building the solution internally [9]. This will enable PaaS cloud customers to have a deeper understanding of the cloud architecture in order to demand better quality of service from CSPs in terms of security provisions. This need provides a source of motivation for this research by developing a framework that can be used to bridge the gap. The research focuses on developing a security framework which consists of industry standard requirements and a systematic approach to evaluate the security offerings on PaaS clouds. The research also attempts to understand how these PaaS security controls and implementations meet the needs of consumers in providing adequate cloud security in the development of web based/ mobile applications deployed and hosted in the cloud.

In alliance with key security considerations for cloud SLAs, as described by the Cloud Standard Customer Council [10] in providing an adaptive framework which can be used to conduct security analysis of security provisions offered in PaaS cloud models by CSPs.

1.3 AIM AND OBJECTIVES

1.3.1 AIM

The primary aim of this research study is to develop a security framework that can be used to assess security mechanisms implemented on PaaS cloud environments based on cloud customer security requirements. The developed framework when deployed assesses the compliance, capabilities and limitations of the security mechanism implemented on the PaaS cloud environment. The framework deployment attempts to test the effectiveness of the framework in capturing customer security requirements in the evaluation and assessment process.

To fulfil these aims, the objectives of the research are as follows:

1.3.2 OBJECTIVES

Objective (a) Critical evaluation of PaaS cloud architectures

Platform-as-a-Service cloud delivery model presents a complex architecture which needs to be broken down and understood in order to evaluate security requirements that are expected to be met by security methods and controls. The goal of this objective is to critically evaluate various PaaS cloud architectures in an attempt to segregate the cloud architecture; understand how components within the cloud function, as well as security risks associated with the cloud components. The key objectives of conducting an architecture review are to evaluate an architecture's ability to deliver a system that fulfils the stakeholders' security requirements and to identify potential risks on each component of the PaaS cloud architecture [11] [12].

Objective (b) Security requirements mapping and classification

This objective focuses on the gathering of cloud customer's security requirements with the use of industry security domains that govern operational security in cloud computing environments. The objective is to categorise customers' security requirements into domains and classify their security demands based on factors and concepts that influence security requirements.

Objective (c) Security provision mapping and classification

This objective requires the evaluation and analysis of security implementations on PaaS Clouds in order to determine the security provisions, capabilities and limitations offered by a CSP on a given PaaS cloud model. The objective is focused on ensuring components within the PaaS are secured and what security mechanism offers the security defence.

Objective (d) Identify the framework components

This objective describes the use of industry security practices and guideline as baselines for the framework development. It requires the use of security approaches and methodologies to forge the framework development process and categorisation of the framework components. The components are then merged to create the framework.

Objective (e) Deploy developed framework

This objective describes the deployment of the security framework to assess and evaluate security provisions and implementations in PaaS cloud models. Based of scenarios for gathering customer security requirements, the evaluation and assessment results will present findings focused at the overall aim of the study as well as demonstrate the effectiveness of the security framework.

1.4 ORIGINAL CONTRIBUTIONS TO KNOWLEDGE

The original contribution to knowledge are summarized and highlighted below:

- A developed reference model that can be adopted to segregate PaaS cloud architectures into layers in an attempt to identify its components, how these components integrate to provide cloud services and security mechanisms implemented in the cloud. (Chapter 5).
- A framework that is used for PaaS cloud security analysis and auditing (Chapter 5).
- A method for gathering and classifying security requirements and provisions which is used to identify critical security areas of focus on PaaS cloud architectures (Chapter 6).

1.5 RESEARCH SCOPE

The scope of this research is limited to Platform-as-a-Service Cloud environments. The developed framework however is considered suitable only for the evaluation and analysis of the PaaS cloud environment and the security controls implemented on the cloud service. The research scope is in line with the shared security and management responsibilities between Cloud Service Providers (CSPs) and their customers.

Although the security of applications hosted on PaaS clouds are critical to the overall security of the system, software applications depend on the resources provided by the system and as such can take advantage of the security controls provided by the system to help provide a foundational level of protection for the hosted applications [4]. This research study is focused on ensuring cloud customer

security requirements are maintained by the environment surrounding application development and is not focused on developed application related security.

1.6 THESIS STRUCTURE

This section provides a structure for how the thesis chapters will be organised and discuss in summary the contents of each chapter.

Chapter 1. Introduction

This chapter discusses the research project overview. The chapter introduces security issues and concerns in the adoption of cloud computing and progresses to discuss the cloud computing security responsibilities shared between CSPs and customers. The scope of the research is highlighted and narrowed down to security issues, security controls and implementation in PaaS cloud environments due to the broad area of cloud computing and the need for further research to be considered in that direction. The aim and objectives of the research are discussed in detail in the chapter as well as the original contribution to knowledge and the research scope.

Chapter 2. Background and Literature Review

This chapter discusses in detail, cloud computing and its architecture. It discusses in detail, different service delivery and deployment models of cloud computing highlighting the benefits, security issues and challenges.

In this chapter, a generic security model for cloud computing is discussed and described in detail, the role of IT governance and implementation of adequate security controls to meet security requirements in cloud computing.

Sections in the chapter are focused on related work on risks of cloud computing and the various industry standards and frameworks that provide guidelines to implementing information security management in the cloud.

Chapter 3. Security in Platform-as-a-Service

This chapter provides a detailed overview of Platform-as-a-Service Cloud. The chapter focuses on the security and management of this service delivery model as well as the security issues and challenges related to the cloud. Other sections in the chapter discusses PaaS cloud security domains, where reference can be made to categorise the security requirements specifications and security mechanism provisions offered in Platform-as-a-Service Clouds.

Chapter 4. Research Approach and Methodology

This chapter highlights the research strategy, approach and methodology for this research. The chapter discusses, the mixed methodology with relevant justification on how the methodology will enables resolving the gap analysis whilst achieving the aims and objectives of the research study. The chapter focuses on the use of evaluation, simulation and testing methods in the analysis of security mechanisms implemented on PaaS clouds. It also presents the secondary research methods used and importance to the research data gathering.

Chapter 5. Framework Development

This chapter discusses the development a security framework that can be used as a tool to identify, evaluate and analyse security mechanisms implemented on PaaS cloud environments. The framework comprises of industry standard guidelines and security parameters which serve as building blocks for developing the framework which is specific for the security evaluation of PaaS Clouds. Using a taxonomy as a criteria for security requirements, the framework presents a detailed

approach of evaluating how security provisions on the cloud architecture meet industry security requirements. The chapter also presents in detail, the segregation of cloud architectures into layers. This segregation highlights one of the original contributions to knowledge.

Chapter 6. Identifying Critical Security Areas of Focus on PaaS Clouds

This chapter is focused on one of the original contributions to knowledge in this study. It discusses in detail, the development of a security mapping matrix using quantitative data gathering techniques and security classification to identify critical areas of focus and security areas of interest within the PaaS cloud architecture. The chapter describes how the matrix can be put into use to generate substantial and significant data necessary to represent customer security requirements analysis and output.

Chapter 7. Framework Deployment and Testing

In this chapter, the developed framework and processes are put into use to evaluate PaaS cloud models in two separate scenarios. The initial phase of the evaluation involves the segregation of the PaaS cloud models into layers while the latter phase produces security evaluation and assessment of customer requirements and also security features and provisions offered within each security domain of the PaaS cloud models. The security assessment also explore vulnerabilities in the security implementations within the cloud architectures.

Chapter 8. Analysis and Findings

In this chapter, a detailed analysis of results from the evaluation and security assessment are analysed in detail in relation to the security vulnerabilities in the PaaS cloud models. A critical analysis of how the security implementations meet the customer requirements are also presented based on evidence established in the simulation, tests and observations.

Chapter 9. Conclusion

This chapter discusses in summary the research study and work done to achieve the aims and objectives raised in the study. The chapter also discusses recommendations based on the analysis of our tests; how security on PaaS clouds can be improved to mitigate security risks. The chapter concludes with a discussion on future work based on this research study.

Chapter 2 : BACKGROUND & LITERATURE REVIEW

2.1 INTRODUCTION

This chapter discusses the evolution of cloud computing, and its adoption and challenges in recent years. It describes relevant studies in the area by providing a detailed discussion of the cloud architecture, benefits, challenges, risks and challenges of cloud service delivery and deployment models. Furthermore, the chapter discusses security governance in the cloud in an attempt to critically analyse industry standard guidelines and frameworks that influence security and management of cloud computing in recent years. Each section in this chapter is designed to discuss both in-depth background and critical analysis on cloud computing security and management. In section 2.2, description of the development of cloud computing and its concept are discussed in detail. Section 2.3 describes the cloud architecture and its service delivery and deployment models. Section 2.4 discusses security issues and challenges of cloud computing while section 2.5 is dedicated to the security standards and guidelines for security and management in information and IT systems. In section 2.6, a security model is presented which highlights the present state of generic security that governs security in cloud computing. The model shows a combination of security governance and the use of technical controls in providing a holistic security management system for cloud computing. Section 2.7 describes security and management responsibilities of various stakeholders in the management of different cloud computing service delivery models. A summary of the chapter is presented in section 2.8.

2.2 CLOUD COMPUTING OVERVIEW

Although there is no universal definition for cloud computing, it can be described as the provision of computer services to multiple users within a virtual environment on a pay as you go basis. It refers to both the application delivered as services over the internet and the hardware and systems software in the datacentres that provides those services [13].Cloud computing allows consumers to access resources online through the Internet without worrying about the technical/physical management and maintenance issues of the original resources [14].Cloud computing is the result of many factors such as traditional computer technologies and communication technologies being provided as a service to customers within a virtual environment and customers only have to pay for the service they need. It developed from technology and business approaches that emerged over the years such as utility computing, grid computing, platform virtualisation, and service oriented architectures (SOA) including the Web 2.0 and distributed systems [15]. All these pre-existing technologies, contributed to the emergence of cloud computing. Hence, Cloud Computing is not a new technology but a new way of delivering computing services via the Internet using distributed systems over virtual architecture.

The cloud itself typically includes large numbers of commodity-grade servers, harnessed to deliver highly scalable and reliable on-demand services [16]. Based on these services, a commonly agreed upon framework for describing cloud computing services goes by the acronym "SPI" [7]. This acronym stands for the three major services provided through the cloud: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). These services are commonly described as a service delivery model and each service provided by a Cloud Service Provider (CSP), requires a different approach consisting of new advances in processors; virtualisation

technology, disk storage, internet connection and inexpensive servers have all combined to make the cloud a compelling solution [7]. Methods of deploying services in the cloud can either be private (hosted within an organisation), public (provided by the CSP and hosted on the internet) or hybrid which combines both private and public cloud architectures. These architectures are referred to as cloud deployment models which can be used to provide any of the service delivery models (SPI) depending on the customers' needs.

The compelling solution offered by cloud computing through virtualisation and delivery of computer services, highlights the benefits that can be obtained from its characteristics and also on demand self-service. These characteristics include the multi-tenancy; which enables sharing of cost and resources by several users' possible, hence improving system utilisation and efficiency. The scalability and elasticity of cloud computing, enables users to increase and decrease their computing resources as needed as well as an on demand self- service attribute, which enables cloud users to obtain and provide additional cloud services themselves without employing the services of an IT administrator.

Although cloud computing is still emerging, the SPI (SaaS, PaaS, IaaS) models have been largely agreed as the major service delivery models of cloud computing. However cloud computing can offer more services where anything can be offered as a service (XaaS), from application services to security services. The SPI and the cloud deployment models both make up the architecture of cloud computing.

In the next section, the architecture of cloud computing and also the benefits and challenges of cloud computing are evaluated and discussed.

2.3 CLOUD ARCHITECTURE

Cloud computing architecture is made up of both the SPI delivery models (see Figure 2.1) and the cloud deployment models. Access to services offered by providers in the cloud require a range of devices available in recent times resulting in greater use and growth of services within the cloud [7]. Users only require a terminal through a browser interface to access services in the cloud. Mobile devices such as smartphones and tablets connected to a broadband network such as WiFi or WiMAX or standalone PCs connected to a high-speed internet, are able to access cloud resources hosted on any of the cloud deployment models without having to install applications or store data on local machines. Clouds can store huge amount of data which are hosted in data centres and server farms at multiple locations in providing service delivery with different levels of virtualisation technologies.

2.3.1 CLOUD SERVICE DELIVERY MODELS

Software-as-a-Service (SaaS): This is the provision of software applications by the cloud service provider via the internet. This service delivery requires the ability of the client or consumer to be able to access applications hosted by the provider without installing it on a local machine (unlike the traditional software model) with the use of a web browser. This stateless application architecture is paid for by the client on a pay per use, monthly based subscription or in some cases free. The maintenance of the software is managed by the provider and support does not require a license with an upfront cost fee. Examples of SaaS include Google Docs, Apple's MobileMe (iCloud) and Zoho.

Benefits of SaaS

SaaS model supports multi-tenancy which allows multiple users access to applications hosted on the CSP's hardware unlike the traditional IT model where individual customers have to install the application on a local server and is isolated only to the customer. SaaS also benefits the CSP or software vendor by increasing its control over use of the software application by limiting unauthorised duplication and distribution of unlicensed copies allowing the vendor greater upgrade and patch management control [15]. The SaaS model requires a customer to lease an application or software when needed by simply logging in through the web browser without having to install it on the local machine at any time. The upgrading and management of the software is relegated to the vendor and not the customer.

SaaS enables the efficient use of software licenses and reduces overhead of license management. Customers can employ a single license on multiple computers at different times instead of purchasing extra licenses for separate computers that may not be used and thus over-provisioning the license [7].

Platform-as-a-Service (PaaS): In the PaaS delivery model, CSPs provide a platform where application and software developers can access an environment to develop computer applications. Vendors provide application toolkits also known as Software Development Kit (SDK) for developers similar to SaaS model but in this case, the service provided is specifically for developers to develop applications using the vendor's platform to build higher level applications. Developers are also able to deploy their applications to run in the cloud which can be accessed via a URL by the end users. Other services provided include database storage and management, programming language on-

demand scalability and security services. Examples include Microsoft Azure, Google App Engine, and Force.com.

Benefits of PaaS

PaaS delivery model provides a lower cost entry for developers by supporting the whole software development cycle (SDLC) of the Web application, thereby eliminating the need for acquisition of hardware and software resources; hence developers can put their web applications and distribute them on the cloud [14], [15].

The PaaS service delivery model enables software developers to develop and deploy web applications at a low cost as applications required for development are hosted and provided by vendors. This encourages web based application development and reduces the complexity of installing and maintaining infrastructures and software used to develop web based applications.

Another benefit of PaaS is that, application web based vendors can host their applications on a cloud platform to enable other developers have access to use these services as a platform on a cloud environment. Therefore enabling developers gain control of the application, whilst using the cloud platform to develop their applications.

Unlike the traditional IT model which supports use by a single isolated user or group, PaaS support multi tenancy which enables multiple users (developers) access to the cloud platform environment. This is done by creating multiple instances of virtual machines to be allocated to multi-users on the same infrastructure.

Infrastructure-as-a-Service (IaaS): This cloud service delivery model describes a service where vendors or CSPs virtually provide the infrastructure to run the entire clients infrastructure. Services such as storage on servers, disks space, backups, security on servers are virtually handled by the vendors and all that is needed is the client to log into the cloud through a web browser and have access to these computer resources infrastructures on a pay as you go. Clients only have to pay for the amount of space they need and need to worry about constant backups or threats that could affect a data centre on site or the cost of maintaining multiple servers. Examples include Amazon EC2, Sun's Cloud services and Google Drive.

Benefits of IaaS

One benefit of IaaS is the ability to reduce cost on data storage infrastructures such as servers and data centres. Users do not need to have a physical storage but a virtual one which serves the same purposes. IaaS enable users to pay only for the requirements they need which include storage disk space and memory on a pay as you go basis.

Alternatively, users can increase and decrease the need for infrastructural services depending on their specific needs at any time they choose to. Hence lower the costs that allow expensing service cost instead of making capital investments [17].

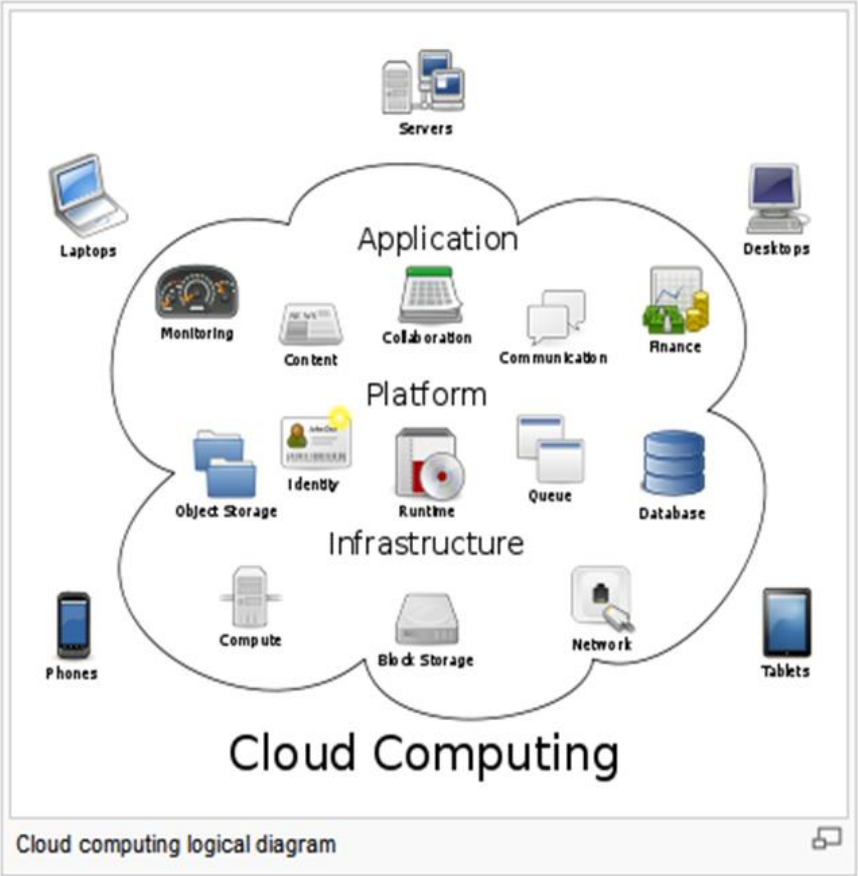

FIGURE 2.1: CLOUD COMPUTING SERVICE DELIVERY MODELS [18]

2.3.2 CLOUD SERVICE DEPLOYMENT MODELS

The cloud services delivery model (SPI) shown above can be deployed on any type of deployment model to users or customers depending on the requirements and specification of the end users' needs. This illustrates the services could be deployed for individual use, corporate use or the general public. Therefore the management of the cloud vary between deployment models. From cloud delivery models fully managed and hosted by CSPs to unmanaged ones managed by individuals or corporate organisations on premises and semi-managed, where management responsibilities are shared between cloud stakeholders. Depending on the structure of internal or external use and of course payment for the services, cloud services can be deployed solely for an organisation or

corporate need (private cloud) or the general public (public cloud) (see Figure 2.2). Hence, SaaS, PaaS and IaaS can be hosted on either a private, public or hybrid (combination of both private and public) clouds.

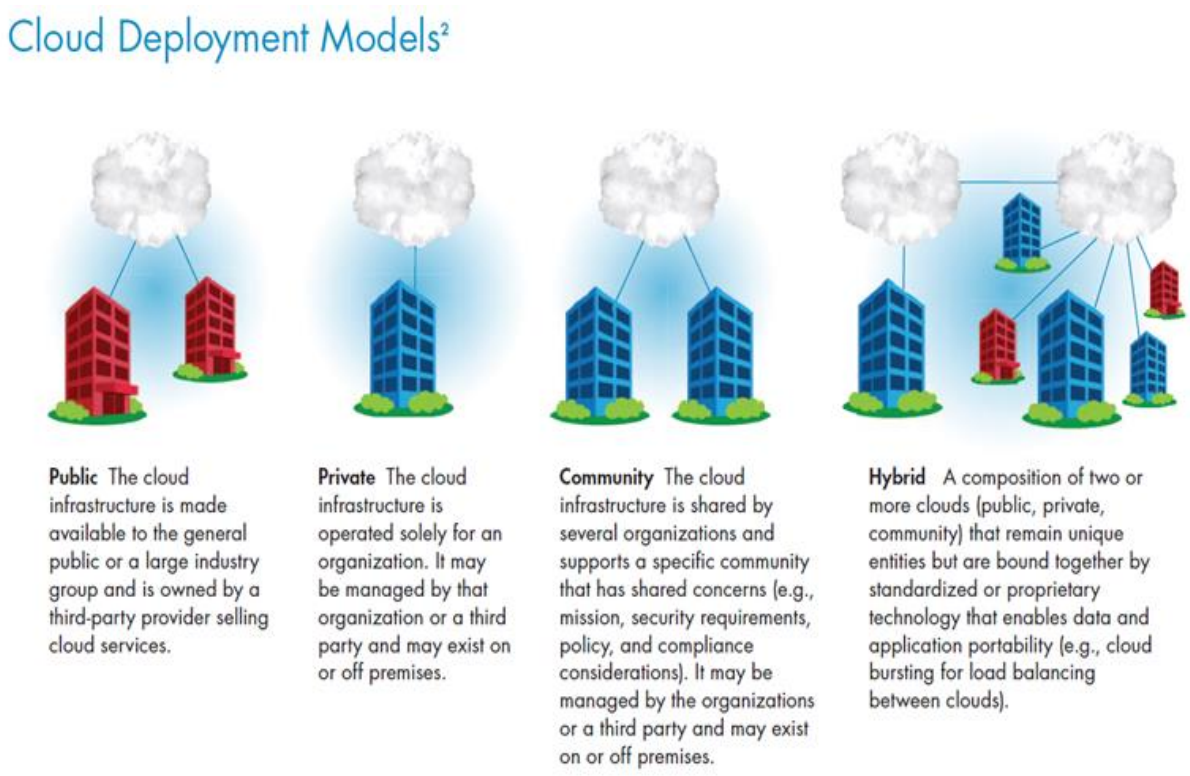

FIGURE 2.2: CLOUD SERVICES DEPLOYMENT MODELS [19]

Private Clouds (Unmanaged): This cloud model provides a customer or organisation with the responsibility of management of cloud services hosted by the vendor or hosted by a vendor bound to a contractual agreement and policies setup by the customer or organisation. For example, an organisation can lease a data centre from a vendor and store resources on it which are very confidential to the organisation and its staff. Such an Organisation will request to have full control of managing the storage hosted by the vendor but will pay for just the infrastructure which will be

cheaper compared to having a large office space full of storage servers. Private clouds can also be developed and managed by organisation using existing software and hardware configurations to developed cloud based services specific for the organisation's needs. A good example is using Microsoft's System Centre packages to develop in house Platform-as-a-Service cloud environments.

Public Clouds (Managed): A public cloud is hosted, managed and operated by a vendor or CSP from one or more data centres and provided for multiple clients [7]. It generally features customers from more than one Organisation sharing the same data centre or infrastructure with each other, which is known as multi-tenancy [20]. The security management of the private cloud is solely managed by the vendor. Customers pay for or lease the cloud services, with no knowledge of its security management and trust the vendors to manage that giving customers, limited control of security patches in the cloud. Most SaaS are hosted on public clouds. Examples of public cloud service providers include Amazon Web Services (AWS), Windows Azure, Google App Engine and Salesforce.com.

Hybrid Clouds (Semi- Managed): This cloud deployment model consists of both private and public cloud services an organisation or customer has access to and is hosted by a CSP. It comprises of a mixture between private, community, and/or public clouds; which is important to support higher resilience, availability, and reliability [21]. An organisation may choose to have sensitive resources available and accessible on a private cloud and also require a public cloud service for other purposes. For example, an organisation may want to provide the infrastructure for storing their cloud application and on the other hand require the web application to be hosted by a vendor. Hence the application is hosted publicly while the infrastructure is in-house. Examples include Amazon Virtual Private Cloud, Amazon Direct Connect, Skytap Virtual Lab and CohesiveFT VPN-Cubed which are

hybrid clouds that work by creating IPSec VPN tunnelling capabilities to connect public cloud physical resources to private cloud resources [22].

Community Clouds: The cloud infrastructure is shared by several organisations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organisation or a third party and may exist on premise or off premise [15]. The defining factor for the community cloud is that different organisations are all assembled for the same cause and share resources towards this common cause[23].

Although cloud computing is still emerging, many users and corporate organisations are embracing the benefits it offers and adopting the cloud computing architecture and services offered by numerous cloud service providers using IT goals to achieve their business objectives. However, the security challenges and risks associated with traditional IT models are also prevalent in cloud computing and addressing these challenges are top priority to providers and customers alike.

The following sections will discuss the security risks and challenges of cloud computing in detail. A detailed look at industry security frameworks and guidelines presently adopted to address issues, risks and challenges with reference particularly to information security management and information security governance are critically analysed.

2.4 CHALLENGES AND RISKS OF CLOUD COMPUTING

The adoption of cloud computing innovation is still in its initial stage. Although many individuals and corporate organisations are adopting cloud delivery services offered by vendors for their benefits, the challenges and barriers in the adoption of cloud computing is still a major concern for a full scale

global adoption. One of the major barriers to cloud computing adoption is lack of trust in the cloud itself [24]. According to an EU report on the major issues and challenges of cloud computing [25], cloud models and technologies are yet to reach their full potentials and many capabilities to which cloud models are linked are yet to be developed to a full degree where all requirements can be met in relation to cloud usage [21].

Early adopters of new technology innovations have embraced cloud services most of which are offered free of charge. Especially SaaS and IaaS, such as online social networking sites, to share photos and store data, access electronic books and journals, play online games, buy and download music from cloud vendors. Organisations and small scale businesses have also adopted cloud computing to reduce the cost of IT infrastructure. Many developers are now using tools provided on cloud platforms to develop web-based applications.

However, the privacy, confidentiality, integrity, availability, reliability, interoperability, management and legal issues that affect traditional information technology are not limited in cloud environments either. A recent study found a total of 160 different standards covering different aspects of the cloud are currently being deployed or under consideration. Some of them bear strong similarities to one another [26]. From the study, the largest gaps of cloud computing challenges were identified to be in the field of management and IT governance process of the cloud architecture and services provided by cloud service providers. On the other hand, Mather et. al [7] concluded that the technical vulnerabilities of cloud architectures need to be addressed properly to preserve security and privacy of resources hosted in the cloud as well as the transparency of cloud service providers.

The Cloud Security Alliance (CSA), a consortium of vendors and users, published top threats to cloud computing providing context in assisting organisations and customers in making educated risk management decisions regarding their cloud adoption strategies [27]. In the report, the fundamental issues were emphasised based on the characteristics of cloud computing and its on-demand nature and also in relation to the CSA's Security Guidance Report for Critical Areas in Cloud Computing, published a year earlier. Remediation and recommendations were proposed for perceived security threats to cloud computing based on the sensitivity of customer information hosted in the cloud by vendors and external threats as well. However at the time of this study, standardisation of a cloud security framework that would govern cloud computing as a whole was yet to be proposed.

In 2010, Ponemon Institute conducted a survey on cloud users. In the report, 46% of IT professionals responded that their organisations have stopped or slowed the adoption of cloud services because of security concerns, indicating a lot is yet to be done to continue advancing cloud computing adoption[28]. Their findings showed that cloud service providers are not particularly focused on cloud security. Rather their priority is to deliver the features their customers want such as low cost solutions with fast deployment that improves customer service and increase the efficiency of the IT function[29]. Further study in 2012 showed that an average of 4,140 business and IT managers surveyed across Europe and Latin America responded they were not aware of the security offerings provided by CSPs to protect their organisation's data in the cloud[29]. According to the National Institute of Standards and Technology's (NIST) special publication[4], the first step in selecting security controls for information systems is to choose the appropriate set of baseline controls which are based on the security requirements, type of assets and risks to those assets on the information system. It is also important to consider the architecture, performance and potential of the information system which the controls will be implemented on.

It is impossible to have unconditional security on any kind of information system. However, choosing the most adequate security control for an information system can make assets stored or shared within the system very difficult to compromise. In cloud computing, the security controls implemented and integrated is not different from traditional information systems although cloud computing presents different risks compared to traditional information systems due to virtualisation and management control of the architecture. Security management best practices such as the Information Technology Infrastructure Library (ITIL), CSA Cloud Control Matrix based on industry standards such as ISO/IEC 27000 series NIST SP-800 and ENISA, have been adopted by many cloud vendors and customers in managing information security in the cloud. Issues, challenges and risks differ amongst various vendors due to different cloud services they provide and the type of deployment model specified by customers. This also is a major source of concern. The top challenges in no particular order of severity are discussed below.

INFORMATION SECURITY: Confidentiality, integrity, availability, authentication and non-repudiation are measures by which any security architecture is queried. They are described as the fundamental security attributes that can be affected by attacks in the cloud [30]. In cloud computing, CSPs host different organisations resources on the same server (IaaS) due to the scalability and flexibility it provides through multi tenancy. The Cloud Security Alliance CSA[8] describes shared technology issues of the IaaS multi-tenant architecture underlying components such as CPU caches used to host the service, were not designed to offer strong isolation properties. However attacks on the cloud may not result in the compromise of all its security attributes but may be specific to affect one or a combination more than one security attributes.

At the network level in public cloud IaaS architecture, a flawed application programming interface (API) or virtual machine (VM) hypervisor, would enable individual tenants interfere or gain access to other tenants' data in transit. A good example is the Black Hat DC Blue and Red Pill attack on Xen's hypervisor [31]. Without a proper authentication and authorisation mechanism put in place, unauthorised access can permit modification of data by unauthorised users and hence compromise confidentiality. More sophisticated attacks can be initiated through VM relocation attacks. A process that allows a malicious insider to copy a victim's VM to a remote machine or portable storage device. Data integrity requires only authorised users can change data and confidentiality and privacy means only authorised users can read data [4]. Keystroke timing attacks as described by Song et al. [32], which describes an attack which occurs when an attacker attempts to steal login credentials by eavesdropping on their keystrokes over the network. The possibility further discussed in a cloud environment [30], can occur over a secure shell (SSH) where the attacker's goal is to measure the time between keystrokes while the victim is typing a login credential such as a password.

Availability describes the process were resources hosted in the cloud are available when needed. Since migration to the cloud suggests organisations' information are not on site and stored in CSPs data centres and server farms, which are also physical locations, environmental and natural disaster also pose a threat to critical information stored at these locations which can affect business continuity. A vulnerable hypervisor can be subject to a distributed denial of service (DDOS) attack and disrupt availability of the service delivery model. A DDOS attacks are the most dominant attacks in the cloud [8], [30]. Once a DDOS attack occurs, data may not be available to the authorised users, thus violating the availability attribute [30]. On the other hand integrity and confidentiality may not

be affected by the DDOS attack. Therefore ensuring that data resources are made available and downtime reduced through data recovery and backup procedures needs to be put in place.

INTEROPERABILITY: Application Programming Interface (API) is unique to different CSPs. This makes interoperability difficult during migration from one service deployment to another and likewise between CSPs. An organisation intending to migrate from a private cloud to a public cloud may experience difficulties in integrating their current infrastructure to be compatible with the CSP's existing one.

Developers, who create web based applications on a particular vendor's PaaS using certain toolkits, may experience challenges upon migration to another platform which means customers might be locked in to a particular CSP. This is sometimes referred to as vendor lock in. The need for a polyglot environment where all programming languages can be supported on a particular vendor's environment is still a challenge in cloud computing. There is a need for data access interoperability, a unique interface for accessing diverse databases which is related to a lot of standardisation issues [24].

MULTI-TENANCY: Multi-tenancy refers to the sharing of a group of servers by multiple customers in the cloud[9]. The sharing method involves the creation of single instances for individual customers on the group of servers. In cloud computing, multi-tenancy adds a number of additional security concerns that need to be accounted for. Multiple client instances must be isolated, their data segmented and their service accounted for[33]. Cloud service providers are faced with the challenge of ensuring complete isolation of individual customer instances and that the compromise to one instance does not affect other instances running on their architecture. Instances of customers must

be invisible from each other while ensuring network and communication latency is reduced to improve system performance.

SERVICE DELIVERY AND BILLING: Ensuring value for money and return on investment for paid services are challenges customers are faced with when they adopt the cloud. Compliance regulations by CSPs for downtime, cost of disaster recovery and hidden fees on support are still loop holes not standardised in cloud computing. According to Marks and Lazano[34], "a critical set of potential cloud obstacles include governance, service level agreements (SLA), and the overall quality of service (QoS) assurance". Weak authentication and verification mechanisms used to register users, encourage cybercriminals access to register for cloud services and conduct malicious activities on the cloud. With a valid credit card, anyone can register and begin to use cloud services immediately[27].

In order to address the challenges and risks of cloud computing, it is necessary to understand the fundamental security requirements for adequate security of cloud service delivery models. It is also essential to consider the responsibilities of cloud service providers in ensuring the security architecture and governance is enhanced to limit the barrier to cloud computing adoption.

LEGAL ISSUES: Legislation surrounding datacentres where computer data and cloud resources are stored raises issues and concern about the adoption of cloud computing. Governing laws and jurisdiction of the country, city or state may grant the authorities or courts rights to customer data which are being stored in those locations. Knowing where your data resides and the laws that govern such regions needs to be considered in the adoption of cloud computing. Three key areas where litigation may ensue include personal data protection, contracting issues and liability for illegal data

[35]. The EU Data Protection Act, for example, strives to keep personal information within the European Union. Hence providers with European customers have to ensure customer data are kept within the region as having data outside the region may kick start litigations. This could be quite confusing as cloud storage could exist as a virtualised server or a mirror data storage. Having to pinpoint where the data is actually stored could be an issue. On the other hand, cloud service providers may be held liable for hosting illegal customer data which may not be illegal in the customer's own region. Legislation such as the Sarbanes-Oxley Act in the USA, could affect how certain data hosted in the region should be stored. Moreover, the legislation in the USA does not protect data from a customer's point of view. Customers have no constitutional rights over their data once it is placed in the hands of an external service provider, and the local authorities can request this data without a warrant[36].

2.5 CLOUD COMPUTING SECURITY GOVERNANCE

This section discusses detailed critical analysis of security standards, frameworks, regulations and guidelines that are generally accepted for implementing information security management. These standards have been adopted over the years by organisations to define the governance activities that will address information security to achieve their business goals. However these standards and frameworks have not yet been well adapted to cloud environments, although some of them are considered significant overall and a worthy starting point [23]. Cloud Service Providers tend towards having audits and certifications based on these frameworks. Since some of the standards and frameworks were written pre-cloud computing[37] and designed for the implementation of information security on traditional corporate systems, they serve as baselines for the development of concepts and guidance sufficient to protect and trust cloud computing[23]. Majority of Cloud

Service Providers strive to pass security audits based on these regulations and standards when providing cloud services for their respective customers. They aim to pass security audits based on one standard or regulation or more than one, depending on the type of cloud service being offered by the CSP. For IaaS and PaaS CSPs, gaining certifications through security audits based on industry standards and regulations is a key to customer acquisition based on customer security requirements. It is assumed that CSPs will at least aim to pass security audits based on the ISO 27001 standard[9].

However, there are many factors that govern CSPs' compliance to specific regulations, frameworks and standards which can include the industry security requirements, data types stored and processed in the cloud and the location of the cloud service infrastructure. Therefore, based on these factors, there is no generic security regulation, framework or standard that addresses cloud security and management. On the other hand, cloud computing services are offered via three types of service deployment models as discussed in Section 2.3. Hence security standards, frameworks and regulations that is applicable on a particular deployment model may be considered unsuitable on another. CSPs could aim to pass more than one audit and become certified to meet its security requirements depending on the factor(s).

The following sections discusses these standards, frameworks and regulations in an attempt to critically analyse their adequacies and limitations.

2.5.1 THE ISO/IEC 27000 STANDARDS

The ISO 27000 series of standards have been created and developed by the International Standard Organisation (ISO) and the International Electro-technical Commission for addressing Information Security issues and the development of Information Security Management Systems (ISMS). It consists

of series of major operational standards that are put together in separate documents to address various information security management issues [38], [39]

Amongst the notable Information Security Management Standards (ISMS) in the series include the ISO 27001 and 27002 series. The ISO 27001 standard was published in October 2005, essentially replacing the old BS7799-2 standard. The objective of both standards is to provide necessary requirements for establishing, implementing and the continuous improvement of an organisations ISMS which is influenced by the organisation's business needs and objectives. The 27001 standard describes in detail using a *Plan-Do-Act-Check* cycle model, the requirements an organisation must meet to achieve certification in the development of an ISMS. According to Disterer [39]and Barlette [40], concerns have been raised on the suitability of the standard for Small-Medium sized Enterprises (SMEs) and the fulfilment of the requirement must be developed and implemented based on an organisation's specification.

On the other hand, the ISO 27002 compliments the ISO 27001 by offering guidelines for organisations through the use of controls and policies to address specific requirements identified via a risk assessment. However since the standard provides direction through the use of policies, procedures and controls to mitigate business risks as well as IT system risks caused by vulnerabilities, specific tools and frameworks are needed to evaluate and review if the implemented controls meet the organisation's security requirements.

In summary, using the ISO 27001 *Plan-Do-Act-Check* cycle model requires specific tools not just to implement controls but to evaluate and review if the implemented controls satisfies the organisation's security requirements and the controls are fit for purpose.

2.5.2 COBIT

The Control Objectives and Information Related Technology (COBIT) is a security framework that was created and developed by the Information Systems Audit and Control Association (ISACA) and its IT audit professionals as a provisional guidance for IT-related internal controls[41]. The business orientation of COBIT consists of linking business goals to IT goals, providing metrics and maturity models to measure their achievement, and identifying the associated responsibilities of business and IT process owners[20]. COBIT was specifically created as a guidance to help auditors within a business review IT related control using a set of objectives to achieve business goals through the use of a management framework. It consists of a model to review internal IT controls which are made up of system development, change management, security and computer operations which revolves around security governance.

The essence of COBIT is to provide good practice that will ensure IT objectives meet laid out business goals. Hence for organisations willing to adopt cloud computing, COBIT can be used to set out requirements by the customer to have clear knowledge of what needs to be delivered by the CSP.

For example in cloud computing, COBIT can be used by cloud customers keen on security to set security requirements which they expect the CSP to meet through security provisions in order to achieve success in their organisation. They can therefore proceed the review if the security requirements have been met by reviewing the business goals. However since there are numerous business goals and IT objectives which security happens to be part of, monitoring and evaluating security controls implemented by CSPs to meet IT security requirements requires a tailored suit framework to evaluate if security requirements have been met before reviewing the business goals.

The Information Systems Audit and Control Association (ISACA), released a current guide aligned with the COBIT framework called Cloud Computing Management Audit/Assurance Program. The objective in terms of security is to provide stakeholders with an assessment of the effectiveness of the cloud computing service provider's internal controls and security. However, the scope of the framework is limited to the governance affecting cloud computing, the contractual compliance between the service provider and customer and the control issues specific to cloud computing [4]. Hence before such assessment can be made, it is important to evaluate security requirement areas such as Data management (for data transmitted and stored on cloud systems), Network perimeter security (as an access point to the Internet) and Identity management (if the organisation's identity management system is integrated with the cloud computing system)[42]. The evaluation of these areas however require security expertise as well as frameworks suitable to identifying and evaluating security controls to meet various cloud service models.

2.5.3 NIST SPECIAL PUBLICATION (SP) 800 SERIES

The National Institute of Standards and Technology (NIST) Special Publication 800-53, calls special approaches to managing information system boundaries and lifecycles[23]. With its version 3 and updated version 4, it relates especially to complex information systems such as cloud computing through the management of information system related security risks. The standard presents The Risk Management Framework (RMF) which provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle [4]. The framework provides six steps similar to the *Plan-Do-Act-Check* cycle model of the ISO 27001 standard. The RMF however acknowledges in its fourth step that security controls must be assessed using appropriate assessment procedures to determine the extent to which the controls are

implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system[4].

The standard also acknowledges that for complex information systems, which cloud computing is, stakeholders managing such complex information systems should consider breaking down the system into more manageable subsystems. The publication points out that implementation of security controls within a complex information system can present significant challenges to an organisation. It admits that the security architecture of such systems plays a key part in the security control selection and allocation process of a complex information system.

Hence an approach to implementation, evaluation and assessment of such security controls have to be tailored specifically to meet the security requirements of such complex information systems. In section 2.3.3 of the publication, the standard admits the ever changing technologies and the effect of information system boundaries. It describes complex information systems such as cloud computing as two important concepts. (i) Dynamic Subsystems: This is described as complex information systems that may or may not be managed solely by the organisation or customer and having subsystems which are managed by providers or CSPs. The publication suggests in scenarios like this, the relative trust relationship between organisations and providers will shape how security requirements are met and how security evaluations are performed. (ii) External Subsystems: The publication describes complex information systems that have subsystems which are not controlled by the organisation. Hence the nature of such subsystems are different especially in organisations that employ external cloud computing services. The guideline suggest that there are numerous factors that can complicate trust levels between stakeholders and the consequence of such factors is based on the use of traditional methods of verifying the effectiveness of security controls.

In summary, the NIST Special publication concludes that the customers or organisations in such scenarios would have to either accept the risk or choose not to obtain the service from providers. This scenario indicates a need for a more suitable and adaptive method that puts the customer in control of verifying security controls implemented on the subsystems by service providers.

2.5.4 ENISA

The European Union Agency for Network and Information Security (ENISA) is a European Union (EU) agency dedicated to EU member states and organisations in ensuring good practices are followed in the advancement of network and information security.

In cloud computing governance, ENISA released in 2009, a report on the benefits, risks and recommendations for information security. The report provides a credible guidance for potential and existing users of cloud computing by providing an informed assessment of the security risks and benefits of using cloud computing. Based on a risk assessment and analysis of three use-case scenarios, the report highlights security risks cloud computing is exposed to whilst providing a security assessment and list of recommendations.

The ENISA report highlights that the level of risks in cloud computing can vary significantly with the type of cloud architecture being considered[43]. This implies that the risks on different service delivery and deployment model differ and hence the security approach also will vary. In the report, ENISA identifies 35 risks that affect cloud computing and a host of vulnerabilities which are cloud specific and general information security mentioned revolve around poor or inadequate security controls implemented to provide information security in the cloud. The implementation which is either down to the service provider or cloud customer security responsibilities.

ENISA suggests cloud customers and providers should state clearly their respective security roles and responsibilities in the preservation of information security on cloud computing. The identified vulnerabilities include a poor system for identity and access management which consists of authentication and authorisation. Others mentioned are, the user provisioning vulnerabilities, remote access to management interface, hypervisor vulnerabilities, and poor key management and encryption vulnerabilities. For non-specific vulnerabilities, the report listed operating system vulnerabilities, poor provider selection and application vulnerabilities as significant loop holes to operational security in cloud computing.

However, recommendation and key massages listed by ENISA through its Information Assurance Framework is for cloud customers to assess the risks of adopting cloud services to understand the pros and cons of migrating to a cloud environment. The framework also recommends users to compare different cloud providers service offerings and obtain quality assurance from their selected providers which should be clearly stated out and agreed upon via service level agreements (SLAs). Customers are recommended to ask questions from providers in order to achieve service quality assurance they will be offered through a list of information security assurance requirements. These requirements are grouped into categories with questions on what security offering is provided to ensure information security.

However without a clear understanding of cloud architectures, stakeholders' responsibilities and a method of assessing security provisions offered by providers, customers using the ENISA framework will find the recommendation list exhaustive. In summary, ENISA recommends that further research in certain areas needs to be considered to improve the security of cloud computing technologies. One key area where research needs to be improved includes the development of metrics for security in cloud computing to assess security requirements and also build trust in cloud computing. Another

area of research that has been recommended is the development of techniques for increasing transparency while maintaining appropriate levels of security in the cloud.

2.5.5 FEDRAMP

Federal Risk and Authorization Management Program (FedRAMP) created by the U.S government, is a unified, government-wide risk management program focused on security for cloud-based systems. The program provides a standard approach for conducting security assessments of cloud systems based on an accepted set of baseline security controls and consistent processes that have been vetted and agreed upon by agencies across the federal government[44]. In the Security Assessment Plan (SAP) Template created by FedRAMP, it describes an approach to security assessment, authorisation, and continuous monitoring for Cloud Service Providers (CSP) through the testing of security controls and in the provision of a plan for security control which ensures that the process runs smoothly.

The SAP template document is intended to be used by independent assessors when testing Cloud Service Provider (CSP) security controls. However, with the clear knowledge that not all cloud service models are completely managed by CSPs and certain components of the cloud service architecture are managed by cloud customers, the FedRAMP does not offer a holistic approach in assessing cloud systems or services that have shared security management responsibilities between CSPs and their customers. In cloud service deployment models such as Private and Hybrid Clouds, the evaluation, review analysis and verification of security controls will require specific approaches.

Although FedRAMP provides adequate guidelines for assessing security risks on clouds through the NIST Special Publication 800-144[4], the standard provides guidelines on security and privacy on

public cloud computing only. This however highlights that there are gaps that needs to be filled in the assessment of private and hybrid cloud deployment models.

2.5.6 ITIL

The Information Technology Infrastructure Library (ITIL) 2011 edition, ITIL version 3, provides a more holistic perspective of the full lifecycle of services covering the entire IT organisation and all supporting components needed to deliver services to the customer[45]. As part of the core publications describing IT service management practices that make up ITIL, the publication is described as the core of the ITIL framework. The ITIL security management explains steps and procedures to ensure that effective information security measures are taken in the planning, implementation, evaluation and maintenance of information security. It provides guidelines for industry best practices in the delivery of IT services by an organisation to its customers. The onus of using ITIL framework is to ensure that customers get services they pay for with the right service level agreements (SLAs) in place. The framework further highlights that providers must offer security services which protect customer assets from unauthorised or malicious access, accountability and non-repudiation of service usage as well as create security zones between customer assets and service assets. Therefore both providers and customers must share the responsibility of implementing the ITIL service management framework to ensure service delivery and expectations are met as agreed in the SLAs. Therefore cloud customers need to come up with ways to evaluate security offerings as stated and agreed in the SLAs to ensure security requirements have been met or are being met as part of the ITIL strategy.

Customers are more interested with how service providers can meet service requirements[46]. Therefore customers would evaluate the service levels that the service provider is offering. Providers

on the other hand must put in place a service level management process to gain customers confidence and the ITIL can be used to ensure this. In Thames' publication[47], ITIL can be a valuable benefit to any IT organisation however it is not a direct fit to cloud computing management. The ITIL framework can be used to identify gaps in cloud computing however various types of cloud service delivery and deployment model suggests ITIL needs to be revamped and its capability extended to incorporate these types of cloud services[45]. The framework has also been suggested to be revamped to incorporate stakeholders' responsibilities and control at various phases of the ITIL service management framework.

In summary, the ITIL Version 3 provides high level description of many information technology best practices that prepare information technology for better services and service delivery. However, information technology cannot rest of past accomplishments of ITIL and the framework which provides practices and provide support and integration must adapt as technology advances [48].

2.5.7 CLOUD SECURITY ALLIANCE GUIDANCE

The Cloud Security Alliance (CSA) is a non-profit organisation that promotes the use of best practices for security assurance within cloud computing[37]. It aims to provide education on the uses of cloud computing to help secure all other forms of computing[49]. It is led by a collection of industry practitioners and key stakeholders in the area of information security and IT management.

The CSA published a Cloud Control Matrix (CCM) specifically for cloud computing providers and customers. The CCM provide a control framework that provides detailed understanding of security concepts and principles that are aligned to 13 domains to address cloud computing security[23]. The Control Matrix consists of control baselines such as COBIT, ISO 27002/27002, NIST SP800-53, FedRAMP, PCIDSS and others such as the Jericho Forum. It provides cloud providers and customers

the ability to map the control baselines to each domain as described by the CSA. The CCM provides a starting point for customers to highlight controls, however it is not a one size fit all solution for all types of cloud computing services [23]. This is because security responsibilities differ on several cloud services where security responsibilities are shared between customer and providers.

Although the CSA through its CCM provides a robust overview for ensuring industry standards are tailored to meet security requirements in cloud computing, understanding the relationships and dependencies between cloud computing models is critical to address cloud computing security. Each security control needs to be aligned to the architecture of respective cloud services.

To support that user requirements can be tailored to cloud security offered by service providers, the CSA created a Security Trust Assurance Registry (STAR). This includes guidelines such as the CCM and The Consensus Assessments Initiative Questionnaire (CAIQ), questionnaire which comprises of 140 questions, provided by the Cloud Security Alliance (CSA) for cloud consumers and auditors to assess the security capabilities of a cloud provider. The questions are based on the security controls in the CCM simplified and converted into questions which cover best practices and security control areas of the cloud security guidance. Although the CCM coupled with The CAIQ offers a good starting point for customers to leverage the controls or assertion questions to validate that the provider has these controls in place [50], the architecture of cloud service models are significantly different and customers must be able to map these control assertion questions to subsystems within the cloud architecture. This can only make the CCM and CAIQ useful as without a thoughtful procedure on tailoring answered questions to specific user security requirements, providers and users alike can find the list exhaustive. The CSA in the guidance, admits that it offers an extensive recommendations

on reducing risks when adopting cloud computing but that not all recommendations are necessary or realistic for all cloud deployments [49].

TABLE 2.1: SUMMARY OF INFORMATION SECURITY MANAGEMENT FRAMEWORKS

Framework/ Standards/ Guidelines	Scope	Strengths	Drawbacks
ISO 27001/27002	Information Security Management	▪ Outlines Security Controls. ▪ Offers risk assessment approach. ▪ Compliance with security standards. ▪ Describes need for a security evaluation and assessment program.	▪ Does not focus of security requirements gathering. ▪ Does not guarantee security control efficiency. ▪ No process for verification of effectiveness of implemented security controls. ▪ Not specifically for cloud computing.

Framework/ Standards/ Guidelines	Scope	Strengths	Drawbacks
COBIT	Information Technology Governance	▪ Focuses on metrics and controls. ▪ Deals with security planning and integrates solution to business processes. ▪ Focuses on security planning. ▪ Links business goals with IT goals. ▪ Enables the establishment of security requirements. ▪ Designed to help ensure IT programs are implemented and managed effectively to maximize the investment of technology efficiently	▪ Not designed for security evaluation and assessment. ▪ Effectiveness of security controls is evaluated only by the business objectives and performance. ▪ Not technical driven. ▪ Not specifically for cloud computing.
ITIL	Information Technology Governance	▪ Focuses on IT processes, service level objectives and SLAs. ▪ Compliance with regulation standards. ▪ Based on the principles of ISO 27001 series.	▪ Must be adapted to suit the organisation's needs and requirements. ▪ Needs to be adapted to suit cloud computing environments.

Framework/ Standards/ Guidelines	Scope	Strengths	Drawbacks
NIST	Information Security Management	▪ Offers risk management approach. ▪ Assists in the selection of security controls. ▪ Allows organisations to tailor assessment procedures and criteria to the characteristics of the IT environment. ▪ Provides guidance and strategies for security control assessment. ▪ Provides guidance for effective assurance of security controls. ▪ Serves as baseline for evaluation and assessment of security controls. ▪ Enables adequate security requirements gathering. ▪ Is adapted to suit cloud computing environments. ▪ Enables security requirements gathering.	▪ Requires the need for additional strategies for the selection of tailored security controls. ▪ Does not provide adequate strategy for mapping security requirements with security controls for effective security assurance.

Framework/ Standards/ Guidelines	Scope	Strengths	Drawbacks
ENISA	Information Security Management	▪ Offers risk assessment approach. ▪ Designed to prevent compromise of information security. ▪ Offers security controls based on industry standards such as the ISO 17799. ▪ Offers strategy for mapping risks suited to specific threats as identified by organisations. ▪ Adaptable for Cloud Computing environments.	▪ Does not provide strategy for mapping risks identified through the risks assessment to components within the cloud architecture. ▪ Does not provide strategy for security requirements gathering.

Framework/ Standards/ Guidelines	Scope	Strengths	Drawbacks
FedRAMP	Information Security Management	▪ Designed to suit cloud computing environments. ▪ Offers risk management approach. ▪ Provides approach for assessing and monitoring compliance with industry standards. ▪ Based on the ISO 27001/27002 and NIST technical standards.	▪ Standardized security requirements which are not tailored to suit organisation's requirements. ▪ No strategy for measuring the security level of standardized requirements. ▪ Standardized requirements could be obsolete. ▪ Is not suited for dynamic nature of Cloud Computing delivery and deployment model.

Framework/ Standards/ Guidelines	Scope	Strengths	Drawbacks
CSA Guidance	Information Security Management	▪ Specifically designed for cloud computing. ▪ Provides strategy for cloud transparency. ▪ Provides strategy for customer assessment of cloud security provisions and offerings. ▪ Promotes the use of best practices for providing security assurance within Cloud Computing. ▪ Based on industry standards which include ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum and NERC CIP. ▪ Provides security controls across several domains.	▪ Security recommendations are not realistic to achieve on all deployment models. ▪ Does not provide strategy for security requirements gathering. ▪ Does not provide strategy for security control evaluation and assessment.

2.6 GENERIC CLOUD SECURITY MODEL

Security requirements in the cloud are characterised by having security standards and policies that govern security, roles and responsibilities of stakeholders involved in ensuring that the security requirements are met. It also includes the service level agreements, risk assessment analysis, security controls and auditing techniques that ensure compliance and security implementations are met according to specific industry standards. A generic cloud security model revolves around all cloud deployment models and service delivery models offered by the CSP. It ensures that the information security of data and assets that reside in the cloud are protected from perceived threats by offering guidance for security requirements in cloud environments.

According to the CSA[27], this model can be grouped into two domains which highlights the areas of concern for cloud computing. The Governance domain which consists of guidance with governance and risk management, compliance and audit, information management and data security, legal, portability and interoperability issues. The Operational domain is however focused on more tactical security concerns and implementation within the cloud. Each domain however consists of recommendations and guidance on how to address the issues focusing primarily on the roles each stakeholder has to play to ensure compliance and customer satisfaction beyond the architecture requirements of the cloud. This ensures that customers can demand better service and CSPs alike can provide quality service delivery by addressing the issues raised.

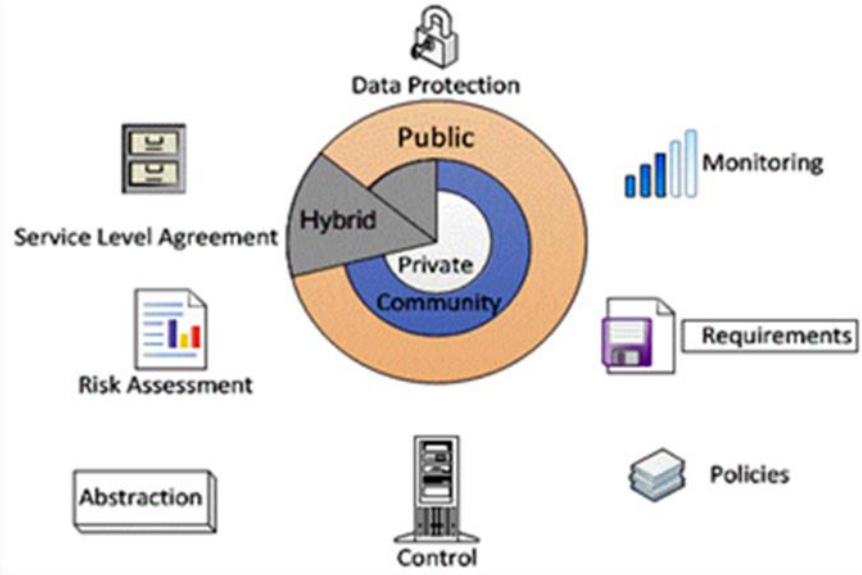

FIGURE 2.3: GENERIC CLOUD SECURITY MODEL

Service Level Agreement (SLA): A SLA is a formal contract used to guarantee that consumers' expectation of service quality can be achieved [51]. In a study by Verma [52], SLA is defined as an explicit statement of expectation and obligations that exist in a business relationship between two organisations; that is, a service provider and a customer. A SLA is drafted to improve relationships between both parties where service level objectives are specified according to a scope and jointly agreed upon.

Therefore, a comprehensive SLA can be different between both parties depending on the services rendered by a specific provider to a specific customer. In cloud computing, a close examination of SLA use cases of the most famous CSPs such as Amazon Web Services and Windows Azure[51], revealed that service commitment by providers is focussed specifically on the annual uptime and availability of the services with little or less commitment on security. For instance, Amazon's EC2[53] describes its SLA as a policy governing the use of Amazon Web Services under the terms and

conditions between AWS and the customer as a service commitment to provide at least 99.95% of annual service uptime provision and offers credits in terms of service downtime with no detail on security as a service.

Policies: Industry-accepted security standards, regulations, and controls frameworks such as the ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum and NERC CIP all provide similar guidelines to provide information security within business organisations and service providers. The Cloud Security Alliance (CSA), a consortium of organisations and security experts, published a Cloud Controls Matrix (CCM) which is a baseline set of security controls using the set of these existing security standards, regulations and control frameworks to assist organisations evaluate cloud providers and guide security efforts. In addition, the Cloud Control Matrix (CCM) provides fundamental security principles to guide cloud vendors and prospective consumers in assessing the overall security risk of a cloud provider, thereby establishing a strong trust level between the two and establishing a market reputation of the provider[54].

However, the CCM is focused much more on compliance as it allows the customer negotiate with the service provider in drafting of SLAs. It helps strengthen trust and facilitates transparency between both parties in an attempt to provide a standard for security measures by providing control specifications by recommending industry standards to its control domains. Therefore it offers a list of requirements and controls they would suggest their cloud service provider to implement [50] but does not provide specific technical details of the kind of controls or where they should be implemented in a cloud service delivery model. SLAs are categorised under the CSA's governance domain.

Controls and Abstraction: Security controls, mechanisms and solutions implemented in the cloud are no different from those implemented on traditional IT systems. The difference however is the implementation and configuration of these controls and how they are integrated to meet cloud computing security requirements. Abstraction on the other hand refers to the process of hiding core components of the hardware by providing layers of representation similar to the component itself. The concept of abstraction is fundamental to computer science, and examples can be found in other software systems such as compilers, databases, and file systems[55]. For instance, a hypervisor provisions abstractions of virtual machines and virtual networks to the end user. A detail discussion of cloud computing security and management is provided in Section 2.7. Controls and abstractions can be categorised under the CSA's operational domain.

Risk Assessment: This can be described as the process of recognizing or finding risks that could affect the achievement of stated objectives [39]. It involves the analysis in order to understand the likelihood and impact of certain risks to determine whether it could be accepted or mitigated.

In cloud computing, assessment of the risks of a cloud service delivery model offered by a CSP is a good indication for drafting SLAs, implementing policies and security controls to mitigate such risks. Risks can be categorised as high, medium or low. Risk assessment can be categorised under the CSA's governance domain.

Requirements: This describes the specific service and security functions that the cloud service must perform through its design. This requirements can be considered as security as a service. Basic security requirements are implemented at the design phase of the system development lifecycle of the cloud service. These requirements include the ability of the cloud service delivery model to

withstand attacks or recover as soon as possible from potential attacks without compromise of the confidentiality, integrity and availability of the cloud service or assets stored, transmitted or processed in the cloud. In a systematic review by Iankoulova and Daneva [56], cloud computing security requirements were categorised into 9 groups. These are access control, which includes identity and access management, attack and harm detection, integrity, privacy and confidentiality, security auditing, non-repudiation, security auditing, recovery and prosecution.

Monitoring and Data Protection: Data monitoring and protection in the cloud involves the compliance of data protection laws and legal requirements by cloud service providers. Depending on the type of cloud service delivery used, the cloud provider's responsibilities could include providing infrastructure, physical security of the premises, operating system and network security. The cloud customer, on the other hand, will be the data controller, actively processing the data for its own business purposes. Depending on the service model used, responsibilities could include controlling the virtual infrastructure and any application security[57]. Consistent monitoring of the cloud service by the customer and cloud service provider needs to be maintained at all times to ensure no security breach and details of the SLA are met. A description of security management in the cloud typical to cloud delivery models is presented in section 2.7.

Figure 2.3 shows the generic cloud security model that is made up of governance and operational domains which revolves around the different types of cloud deployment models. Our focus is on the controls implemented on public clouds and developing a framework that can be used to evaluate the security offered by CSPs in this generic cloud security model on PaaS public clouds.

2.7 CLOUD COMPUTING SECURITY AND MANAGEMENT-RESPONSIBILITIES AND ISSUES

The level of responsibility a cloud service provider takes on depends on which cloud service model and deployment model is chosen by the cloud service customer. Customers must not solely rely on cloud providers for security but must take a different approach to security by applying security best practices to ensure security on the selected cloud models[9]. The problem at the moment is that service level agreements (SLAs) provided by CSPs to customers are centred on service related aspects such as availability and performance, and very few terms are related to security[58]. However, it becomes difficult for cloud customer, or their agents, to audit the services provided by CSPs[59]. The boundaries between these responsibilities is not always clear cut, and can depend on the agreement signed by the customer and other factors[37]. Therefore having a full understanding of stakeholders' responsibilities in the management and security of cloud service delivery and deployment models is a huge step forward in applying best practices and ensuring accountability of not just quality of service rendered but also security implementations put in place in cloud architectures. Figure 2.4 shows the various cloud service delivery models and the stakeholder responsible for the management of the service. Unlike traditional IT systems, where the IT administrator is responsible for providing security and management of the entire architecture, cloud computing offers shared management between stakeholders involved. However, this shared management responsibility is typical for public cloud deployment models as illustrated by CSPs.

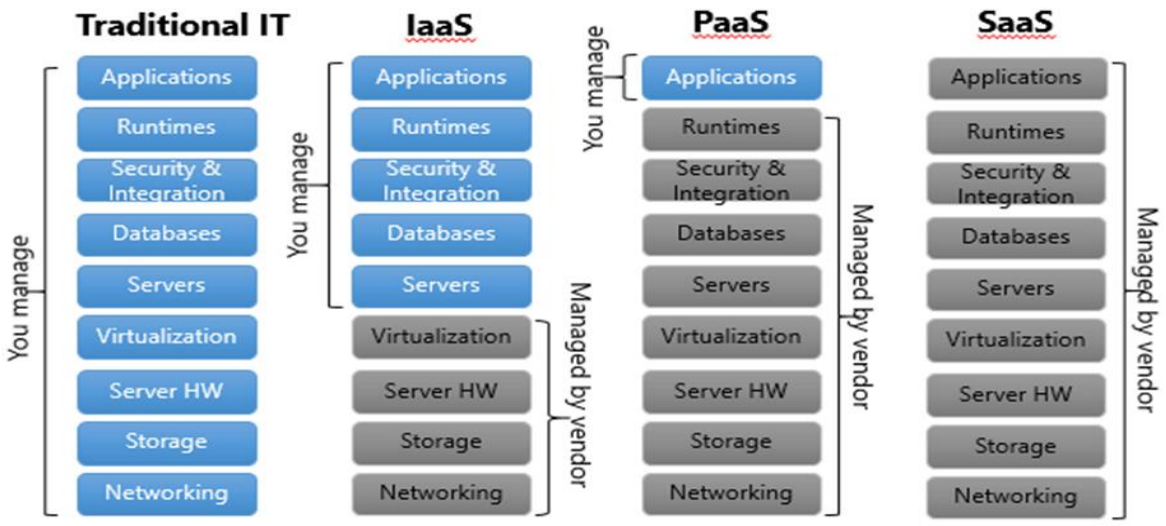

FIGURE 2.4: CLOUD COMPUTING MANAGEMENT[60]

2.7.1 SERVICE LEVEL AGREEMENTS (SLAS)

Service Level Agreements (SLAs) can be described as a contractual agreement that guarantees minimum Quality of Service (QoS) and clearly set of expectations for that service between a Cloud Service Provider (seller) and Cloud Customer (buyer)[10][22]. It can also be described as a formal agreement between two parties sometimes called a service level guarantee designed to create a common understanding about services, priorities and responsibilities[61][62].Given the global nature of the cloud, SLAs usually span many jurisdictions, with often varying applicable legal requirements, in particular with respect to the protection of the personal data hosted in the cloud service. Furthermore different cloud services and deployment models will require different approaches to SLAs, adding to the complexity of SLAs[63].

On the other hand, different types of cloud customers from single to multiple users and small businesses to large organisations determine how service level objectives are defined which are clearly

laid out in different types of SLAs. SLAs are also drafted based on the security responsibility of both stakeholders in ensuring security objectives and requirements are met depending on the level of control. In Cloud Computing security, SLAs are established based on the level of security offered by the provider and also the security level expected and requested by the customer. A customer must understand his security requirements and what controls and federation patterns are necessary to meet those requirements. A provider on the other hand, must understand what they must deliver to the customer to enable the appropriate controls and federation patterns [48]. Customer requests and expectations are clearly influenced by how the security level of the cloud service model can affect business assets and business objectives. These objectives can be defined as the security requirements of the cloud customer which are expected to be met by the providers as described in relevant SLAs. Considering different types or users and service cloud models, SLAs could come in various types. The current market offers two types of SLAs for customer's specific requirements[64]. These are categorised into negotiable and non-negotiable SLAs.

Non-Negotiable SLA- A non-negotiable SLA is described to be less expensive than a negotiable one but is not acceptable to customers with critical applications and data [64]. However it is offered by most CSPs of public clouds as a one size fit all policy where customers can receive a form of compensation if service needs described in the agreement are not met by the CSP. When this type of SLA is offered, the CSP administers those portions stipulated in the agreement [65] and customers have to continuously be on the look out to ensure the service agreements are met. If not satisfied, customers could choose to stop using the service, however they cannot negotiate the terms to suit their own needs with the CSP. The offerings in this type of SLA is static and does not address the individual needs of every customer. A consequence which is described as customers having a limited

set of offerings in terms of security features, often without knowledge of how such security mechanisms are implemented[58].

Negotiable SLA- This type of SLA is described as one where the rules for the negotiation are established including the option to negotiate manually, and a template with the stakeholders where the negotiated parts are clearly expressed [66]. In Cloud Computing, negotiable SLAs are more like traditional information technology outsourcing contracts. They can be used to address an organisation's concerns about security and privacy policy, procedures, and technical controls[4]. This type of SLA is more applicable to organisations with critical data and applications and compromise of such data may affect the organisation significantly. The outcome of the negotiation however depends on the size of the organisation and the influence it can exert[4].

Although the negotiable SLA may contain numerous service level objects which the customer may want to negotiate with the CSP, the importance of computer systems security, its intricate characteristics and the growing of outsourcing scenarios, including the outsourcing of security services, security service levels need to be agreed[67]. This will include who is responsible to implementing security features and who would assume responsibility when a problem occurs. Therefore the core fundamentals of customers negotiating SLAs is down to security. It is specific to deal with metrics related to security requirements or demands which include security mechanisms such as cryptography, data packet filtering, redundancy of hardware and software, security backup policy and protection against malicious attacks[67].

2.8 SUMMARY

Cloud computing is an emerging technology that spans across providing computing resources to a wide industry of businesses and academic users. Governed by policies, frameworks and publications that provide guidance to its security, the challenges and risks to its promising future revolves around security management of the environment's architecture and responsibilities of its stakeholders. These standards and guidelines only offer direction in IT governance, risk assessment and ensuring good practices are followed in regards to security in the cloud. The service level objects offered by CSPs and understood by customers have to be agreed and clearly documented through service level agreements. Although cloud computing offers several benefits which includes return on investment and increased performance, security of the cloud architecture and customer data are faced with growing security threats, challenges and issues. With the use of industry standards and guidelines, it is certain cloud customers must work closely with CSPs to ensure security and management responsibilities are clearly stated and met. A cloud security model which embraces industry guidelines and standards needs to be developed to ensure security management specific for customer data and varying cloud architectures.

Chapter 3 : SECURITY IN PLATFORM-AS-A-SERVICE (PAAS)

3.1 INTRODUCTION

Platform-as-a-Service (PaaS) service delivery model describes an environment where a developer can create customised applications within the context of development tools that the platform offers [15]. The environment allows developers to deploy developed applications using specific development languages which the CSP offers on the platform. In the PaaS service delivery model, CSPs offer customers a subscription where application and software developers can access an environment to develop web based applications. Service provided can include an application toolkit also known as Software Development Kit (SDK) which is downloaded and installed on the client machine or can be web based. The SDK serves as the code building blocks and consists of programming languages and applications which are used to initiate the developer's environment to develop applications. Once the applications are developed, the customer can also deploy the application to be hosted on the CSPs web/application server using the subscription credentials.

The deployed applications run in the cloud which can be accessed via a URL by the end users for which the application is built. Other services provided include database storage and management, programming language on-demand scalability and security services. Although the first generation PaaS CSPs such as Google App Engine, Windows Azure and Force.com, required that customers use specific programming languages on their platforms, other CSPs have emerged who support the use of multiple programming languages on their PaaS cloud service. Examples include OpenShift and Cloud Foundry.

PaaS delivery model provides a lower cost entry for developers by supporting the development of web/ mobile applications, thereby eliminating the need for additional acquisition of hardware and software resources; hence developers can put their web applications and distribute them on the cloud [7],[16]. The PaaS service delivery model enables application developers to develop and deploy web applications at a low cost as software required for development and environment for deployment are provided by the vendors. This encourages web based application development and reduces the complexity of installing and maintaining infrastructures and software used to develop web based applications.

This chapter discusses Platform-as-a-Service (PaaS) security and management as well as a detailed background on some of the issues and challenges that surround the cloud service. It also discusses the industry security requirements that are expected to be met through security controls and policies implemented on the service delivery model. The chapter also discusses related works and research that have already contributed to the evaluation of security and security provisions and implementations in cloud service models including PaaS clouds.

3.2 PLATFORM-AS-A-SERVICE SECURITY AND MANAGEMENT

The cloud service customer and cloud service provider have a shared responsibility for securing the cloud services, when leveraging the cloud[9]. Depending on the nature of the deployment, new risks are introduced and ownership of controls and management will shift between providers and customers alike[23].

In PaaS Clouds, security and management shift between cloud customers and providers depending on the cloud deployment model which could be Public, Private or Hybrid. The amount of

responsibility shouldered by each party can change depending on the model adopted[65]. Hence, the sensitivity of the data being stored as well as the target industry are significant factors that determine what type of PaaS cloud service deployment model customers' purchase and the level of their security expectations. For instance, the security and management of a Public PaaS Cloud is significantly different compared to a service deployed on Private or Hybrid models. In Public PaaS Clouds, the cloud service provider is responsible for the security of the components of the cloud. The CSP manages the underlying infrastructure, networks, storage devices and operating systems. Tasks like monthly security patching, logging, and monitoring, scaling, fail over, and other system administration related tasks are provided by the vendor. This type of PaaS cloud model is called "***Managed PaaS***", hence it is managed by the provider.

In Private PaaS cloud environments, the customer is responsible for the security of the underlying infrastructure as well as the security and management of the cloud components. CSPs do not provide the abstraction of the infrastructure as customers have access and control to the underlying platform resources. This is also known as ***"Unmanaged PaaS"***. The customer is responsible for the entire security implementation and configuration on this cloud and has complete control over the underlying infrastructure and software. However, security provisions and their capabilities once implemented are provided by the CSP as security features in such on-premises clouds.

In Hybrid PaaS Clouds, providers are responsible for security and management of the PaaS components, however the underlying infrastructure as well as data storages are managed by the customer. It offers the capability to deploy the PaaS software on both a private and public cloud but at the sacrifice of requiring the customer to manage the application stack and underlying infrastructure or resources[9]. In some Hybrid PaaS clouds, its architecture comprises of having

certain services within a Private PaaS cloud outsourced to be managed by a CSP or cloud vendor. This type of PaaS cloud model is also known as Semi-Managed PaaS, because both provider and customer share the responsibility of cloud security and management.

Therefore, cloud service providers depending on the service they provide or customer base, need to come up with different service level agreements (SLAs) or terms and conditions of their security management in regards to customers' security expectations. In most cases, organisations and businesses tend to adopt the Private or Hybrid PaaS Cloud services. This is typical as they require a higher level of security and relatively hold data they consider sensitive or are subject to government regulations to provide data confidentiality and avoid security breaches. On the other hand, customers who provide web based application or services such as social media data or a start-up or smaller company, may be very risk tolerant and rank getting their web application services running at a low cost as a higher priority than investing in security and will considerably adopt a Public PaaS cloud service[9].

3.3 PLATFORM-AS-A-SERVICE CUSTOMER TYPES

Corporate Customers: Cloud corporate customers in this category include private and public organisations, educational systems, government organisations, small businesses and multinational corporations. They constitute multiple or group of users and IT administrators that handle certain cloud service management roles and resources such as development of end user applications. Private and Hybrid PaaS cloud service models are common amongst large corporate cloud customers with small businesses much inclined to public cloud models during start-ups. However many large corporations are adopting public PaaS cloud services in the development and production of web based applications.

Individual Customers: Customers in this category include non-business or commercial cloud users such as single application developers and cloud enthusiasts. This type of customers do not own on-premises infrastructures or datacentres which needs to be migrated to the cloud or linked in form of hybrid cloud services. Most single cloud customers subscribe to public cloud service models to provide top to bottom production PaaS cloud resources. On the other hand, single customers could adopt private PaaS cloud models for test bed environments in the development of web applications.

3.4 PLATFORM-AS-A-SERVICE SECURITY ISSUES AND CHALLENGES

Preserving the confidentiality, integrity and availability of data and computer resources are critical security challenges of cloud computing. In addition to these, security considerations on PaaS include access and authorisation issues, working with distributed applications, and storage and data security [4]. Since the scalability of PaaS supports multi-tenancy, which allows many tenants deploy their code and share a common resource pool on a single data centre, security policies regarding how data is stored, secured and shared between multiple customers has to be made very clear[68]. This raises serious concerns when organisations and developers decide to go down the PaaS route.

Since the security implementations on PaaS cloud environments are quite ambiguous and not properly communicated through SLAs and policies, understanding the cloud architecture, its components, security vulnerabilities, security risks, security mechanisms and controls implemented to mitigate such risks, are very significant in the adoption of a specific PaaS cloud platform. The ISO highlights the major security issues of PaaS as security of the PaaS platform itself (i.e., runtime engine), and security of customer applications deployed on a PaaS platform[7]. However, other issues such how data is stored and who has access to the data contributes to the challenges faced by this cloud delivery model.

PaaS customers have to constantly depend on both the security of web-hosted development tools, security of their developed applications as well as the security of the underlying infrastructure on which the cloud platform runs; which they do not have the assurance that the development environment tools provided by a PaaS provider are secure. These security issues are prevalent in cloud computing due to the overwhelming vulnerabilities presented through insecure interfaces and APIs, vulnerabilities in virtual machines, hypervisors, virtual networks, and virtual machine images. As with many evolving technologies, the lack of virtualisation industry standards has resulted in a number of vendor-specific best practices and recommendations that may or may not be applicable to a particular environment. Entities need to understand and evaluate their own environments to identify the unique risks virtualisation brings[69]. The following are detailed description of threats and vulnerabilities prevalent in PaaS Clouds.

3.4.1 PAAS CLOUD VULNERABILITIES

Nature and Characteristics of PaaS Cloud Environments: The cloud's distinctive nature of on-demand self-service requires a management interface that's accessible to cloud service users. The probability that unauthorised access could occur is much higher than for traditional systems where the management functionality is accessible only to a few administrators[70]. When an attacker gets possession of a legitimate client identity by theft or some other means, an authentication attack is initiated[71]. Hence, the nature of PaaS cloud environments like other cloud service models shares a common ubiquitous network access, resource pooling, rapid elasticity, and measured service. On the other hand, PaaS architecture is more prevalent to attacks as it is in the middle of the cloud deployment stack with access one part of the cloud facing an internal backend and the other facing multiple users via public internet.

Core-Technology Vulnerabilities: Web applications and services, virtualisation, and cryptography - have vulnerabilities that are either intrinsic to the technology or prevalent in the technology's state-of-the-art implementations[70]. These technologies have increased the exploitation of design and weaknesses inherent in the architectural design and technological issues relating to distributed integrated systems such as clouds. In PaaS Cloud models, the lack of security reviews at different phases of the security development lifecycle of PaaS cloud environments has created gaps which can be exploited by insider threats or external attacks. For instance, threats such as injection attacks, DDOS attacks and wireless security attacks have increased on cloud architectures due to various communication and network channels prevalent of ubiquitous on-demand technologies implemented on the cloud. On PaaS clouds, the network infrastructure is a significant component of the cloud. Communication between components of the cloud and resources creates an avenue for increased attacks through communication endpoints. The virtualised nature of the PaaS cloud environment also make network security difficult to implement when being compared with traditional distributed environments.

Security Control Defects: The security controls and implementations in the cloud are known to be important in ensuring a holistic security approach is maintained in the cloud. Apart from the core technologies mentioned as a vulnerability earlier, security controls such as cryptography and other security implementations have been fundamental. This is because it is unthinkable without the use of cryptography to protect the confidentiality and integrity of data in the cloud. Vulnerabilities and threats concerning insecure or obsolete cryptography are highly relevant in cloud computing[72].

Inadequate Security Offerings and Implementation: Buyers of commercial cloud services, especially software as a service (SaaS), are finding security provisions inadequate[73]**.** This is also

prevalent in other cloud deployment models such as IaaS and PaaS. Security provisions offered on various PaaS clouds by vendors differ. The ability to scale up security in the cloud can also depend on numerous factors from service level agreements to architecture and nature of the PaaS cloud environment. Security offering adequate to meet the needs of a particular user on PaaS clouds may seem inadequate to meet security requirements of other cloud users.

3.4.2 THREATS TO PAAS CLOUDS

Service- Level Threats: These threats are common to web services components and architectures within the cloud service model. These threats are prevalent on communication interfaces and end point channels of the PaaS cloud architecture. The threats include man-in the-middle, brute force, injection, dictionary attacks and replay attacks. Others are cross-site scripting and session hijacking. The cloud is exposed to these threats due to vulnerabilities or weakness in the cloud design and security control defects in the cloud service model[71]. Other factors include the lack of security awareness during different stages of the development lifecycle of the cloud environment. These threats attack inadequacies found in security implementation used in the authorisation, authentication and access control of user credentials.

Host-Level Threats: The Host on PaaS cloud architectures suggests servers that host web services, applications, operating systems, core kernel technologies and middleware libraries. It also include virtualisation technology hosts and communication channels to and from such hosts. Intrusive malicious software also known as Malware include Trojan horse, Spyware, Worms and Viruses all constitute serious host-level threats to PaaS Cloud architectures. Access control vulnerabilities can allow perceived threats such as eavesdropping due to unauthorised access.

Infrastructure- Level Threats: There are various infrastructures that make up the PaaS cloud model architecture which consists of mostly physical resources that support the network and storage services. Although they consist of physical servers, they constitute the backbone architecture of the distributed system that make up the cloud architecture. Threats to these infrastructures include Distributed Denial of Service Attacks (DDOS), Hacking, Routing Attacks, Man- in- the- Middle Attacks, Spoofing, Eavesdropping and Replay Attacks.

3.5 PAAS SECURITY REQUIREMENTS AND DOMAINS

Security requirements are engineered to specify a systems' security policies and both policies and requirements should address security risks. Security mechanisms are then architected to fulfil the security requirements. Some of these concepts influence the engineering of security requirements, whereas others for instance security mechanisms, security vulnerabilities, and attacks, are influenced by the security requirements[74]. These concepts that influence security requirements by which they are influenced is clearly described in the figure below.

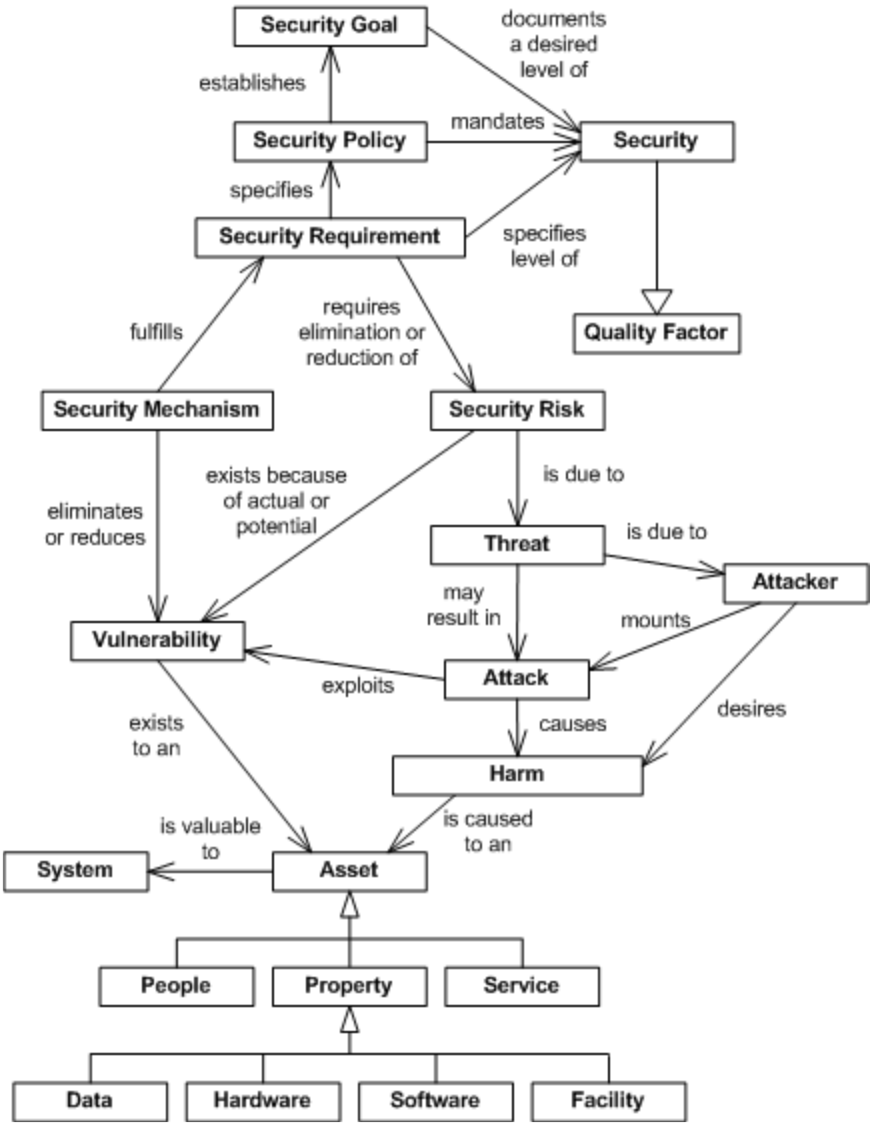

FIGURE 3.1: CONCEPTS THAT INFLUENCE AND ARE INFLUENCED BY SECURITY REQUIREMENTS [74]

The Cloud Security Alliance suggests that with any area of security, organisations should adopt a risk based approach to moving to the cloud and selecting security options[49]. This should include a full risk assessment and a methodology for determining their security requirements. These security requirements are forged from a taxonomy of perceived user needs, security standards and practices and prioritised risk scenarios[75]. Depending on the nature of the deployment, new security risks will be introduced as well as the ownership of security controls will shift which may require more or

different types of controls[23]. However regardless of the nature of deployment, customers must have adequate governance and control over their entire environment. The onus of responsibility is on cloud customers to recognise their compliance objectives and requirements, establish a control environment and meet those objectives and requirements, and then validate that control environment is effective to the appropriate level[23]. Capturing security requirements is considered a tedious task, as good security requirements needs the requirements specified to be aware of the threat environment, regulatory compliance, security policies, security classification, service level objectives and knowledge of evolving security vulnerabilities[71].

On the other hand, protecting and carefully managing customer requirements are crucial for establishing trustworthy Clouds and are the responsibility of CSPs[21]. Customer risks will vary depending on the CSPs and it is difficult for CSPs to meet individual needs of each customer. Hence CSPs try to obtain third party accreditation of their security claims which could relatively be time consuming and expensive[76]. The increase of third party accreditation is much on the rise by CSPs and indicates a good trend in cloud computing security, however what is important is for cloud customers to identify if given PaaS providers meet their requirements and how PaaS Cloud Service Providers rank against other PaaS CSPs.

In disparity to private cloud security, public cloud users do not have the luxury of being able to review details of or examine the security implementation, processes, and procedures of a public cloud. Not only is it not prudent for a CSP to expose technical details of cloud security, it also isn't cost effective to meet the needs of individual consumers by sharing such information to win their business. As a result, the best method of addressing this is to place value in trusted third party accreditations[76].

However, customers still need to evaluate security controls implemented by CSPs to be certain they meet their requirements and mitigate risks that may affect business goals as identified through their risk assessment. It is common for cloud owners to assume that a move to the cloud will in some way reduce the need to validate or verify security controls operating effective[23]. Unfortunately, vendor claims about security are often made without sufficient justification—as the reality of vulnerability exposure and often poor security practices evidence. In addition, many cloud service providers may make vague representations of their security while also transferring all liability to customers[76].

Therefore in PaaS cloud service models, customers need to understand the environment, requirements and risks, define security control objectives as well as verify that controls in place are operating effectively. To evaluate security and privacy requirements, the Cloud Standards Customer Council[10] suggests:

"A critical initial step for ensuring sufficient cloud security is establishing a classification scheme that applies throughout the enterprise, based on the criticality and sensitivity of enterprise data. This scheme should include details about data ownership, definition of appropriate security levels and protection controls, and a brief description of data retention and destruction requirements. The classification scheme should be used as the basis for applying controls such as access controls, archiving or encryption".

Our approach to this classification scheme is presented in Chapter 6. Customer requirement specifications are enormous and could be delegated at different layers in the cloud[21]. These requirements consists of functional and non-functional requirements. Functional security requirements on PaaS clouds describes the security of the system and service operations. It comprises of the service model workflow operations, who has access to each part of the service and the security of the environment where applications are developed and deployed. Non-functional

requirements on the other hand, describes how the service model architecture function on each layer and how they comply with security and privacy of data in transit or at rest. The security requirements that determine the architecture of security solution are: confidentiality, authentication, single sign-on, trust management, monitoring and logging, intrusion detection, data protection and isolation, and denial of service[71]. These requirements have been forged from the CSA's cloud security domains which highlights areas of critical focus where security requirements as identified by customers could be mapped into. Careful categorisation of customer requirements would simplify their management and help in the direction of providing enforcement assurance measures[77]. The CSA focuses security guidance on two broad domain categories of cloud computing environments. The governance domain discusses the policy issues around cloud computing environment while the operational domain discusses the tactical security concerns and implementation within the architecture. Using this guidance, customer in depth security requirements are focused around the operational domain in PaaS, which highlights guidance with in depth security defence mechanisms which are linked to specified security controls.

These security requirement specifications have been carefully identified and categorised based on operational security domains and are the ones relevant to PaaS cloud service models and not all other Cloud Computing delivery models as identified by the CSA Security Guidance. They include Identity and Access Management, Encryption and Key Management, Virtualisation Security, Network Security and Database Security. Each domain in this study has been labelled D1, D2, D3, D4 and D5 respectively.

D1-Identity and Access Management: This requirement domain refers to the security and management of individual identities, authentication, authorisation and access to assets in an information system governed by policies and controls with appropriate privileges within the system. It is concerned with questions on, how is access restricted to protected resources and what kind of controls can be placed on such access? How are identities verified?[78]. In PaaS, customers have access to the environment via a web portal or management API. The whole identity and access management encompasses the ability of the PaaS and controls implemented to confirm and manage the life cycle of an assured identity (human/device/process), assigned properties of entities, manage permissions to perform an action in the cloud and also manage the lifecycle of digital credentials through authentication[79].

This includes the management of the API as well as the security of the web portal interface. In multi-tenant cloud environments such as PaaS, providers must segregate customer identity and authentication information while the identity and access management components should also be easily integrated with other security components on the cloud[80]. Identity and Access Management encompasses the trio of authentication, authorisation and access control of users within the cloud environment and revolves around API management and Web Security. The service model must be able to identity and authenticate authorised customers while keeping out malicious and unauthorised users. Also in the process, it should also be able to ensure the session created by the authorised user is not hijacked before, during or after the authentication authorisation processes have been completed. The management of the API which involves use RESTful or SOAP services to prevent session hijacking and how session keys are exchanged during the authentication and authorisation handshakes between the customer and the PaaS cloud interface. As well as the Web

Security should encompass the security of data in transit or channel during the authentication and authorisation handshakes to ensure the channel or session created is not hijacked or injected by malicious and unauthorised users.

D2- Encryption and Key Management: Encryption of data before storage in the cloud is essential on public clouds due to the multi-tenant model. Ability to utilise cloud storage controls perhaps built in controls to enable encryption and segregation of data. One of the most difficult processes in public cloud computing typical to PaaS, is the management of symmetric or asymmetric keys used in the encryption of data. Maintaining proper key management and storage from unauthorised users is essential for security of data stored on public clouds. Managing access to keys securely is what separates a weak encryption from a strong one. Although data encryption helps protecting data confidentiality, it also obsoletes the traditional data utilisation service based on plain text keyword search. Thus, enabling an encrypted cloud data search service with privacy-assurance is of paramount importance [81]. On the other hand, keeping encrypted copies of same data in the cloud may affect system performance and incur high computational cost[82]. There are several types of encryption that should be considered which include storage, application level, network and edge of the cloud encryption. When strong encryption or cryptography is deployed properly, it is virtually difficult to break even by the most determined attacker[83]. This requirement domain expresses the strength of the encryption methods, access to encryption keys as well security of encryption key storage within the PaaS cloud service model.

D3-Virtualisation Security: Virtualisation is the concept by which cloud computing is established. It is the mechanism that abstracts the coupling between the hardware and operating system [49] by presenting the host platform virtually. It refers to the abstraction of the underlying physical resources

to improve agility, flexibility, reduce cost and enhance return on investment. A virtualised environment ensures that each partition is completely isolated from other partitions; as isolation is a fundamental property of virtualisation[71]. Basically virtualisation in the cloud is of different types which include server, storage and network virtualisation[49]. Having virtual machines run on the cloud brings about various challenges as well. Encryption of virtual machine images to prevent modification and theft at rest or when they are running. Access through virtualisation to resources and service running in the cloud requires protection against failovers through hardware load balancing. However, CSA[49] suggests providers have tried to satisfy virtualisation security as a service on a cloud platform but because these services take many forms and lack transparency regarding deployed security controls, they have caused market confusion and complicated the selection process of adequate controls. Virtualisation takes many forms. System virtualisation, also commonly referred to as server virtualisation, is the ability to run multiple heterogeneous operating systems on the same physical server. Other forms of virtualisation include storage virtualisation and network virtualisation, namely logical representations of the physical storage and network resources[84].

In PaaS cloud service models, virtualisation security encompasses the security of the virtualised host or abstraction of all physical resources that enables the Middle-Tier and Front End stacks to run (storage and network virtualisation). It also comprises of the security of the virtual appliance, which is described as a pre-packaged software image designed to run inside a virtual machine[69]. Security requirement that encompasses virtualisation expresses the need to secure the abstraction from core physical platform resources and ensure isolation of multiple tenants using the same cloud service resource pool. It also expresses the security of the operating system and all other software or physical resources that make up the system. The timely application of security patches to the software and

reconfiguration or replacement of physical resources that host the abstraction layer as areas which virtualisation security covers. Virtualisation security also constitutes file integrity management which is the method of ensuring that files such as sensitive system or application configuration files are not corrupted or changed to allow unauthorised access or malicious behaviour[85].

D4-Network Security: This domain surrounds and expresses security and auditing mechanisms that are implemented to ensure the underlying security of the Front End and Back End architecture of the cloud. This include the security of the physical platform resources as well as the repository database management services. It also includes the security of communication channels and how they interact with the cloud environment. Although PaaS clouds are built upon physical infrastructures which will include traditional networking security implementations, it is important to note that the virtualised services it runs are not as mature as their traditional networking counterparts and it is important to be aware of the current state of these virtualised services and what controls may need to be implemented at the virtualised and traditional network boundary[85].

Network security requirements demand the isolation of networks through Virtual Local Area Networks (VLANs) and tunnelling. It involves the proper segregation of tenants and networks within the multi-tenant architecture. Giving tenants the ability to create applications and application containers from a list of allocated resource pools without interference or data leakage. It involves the appropriate methods of network isolation and segregation which is supported by identity and access management policies put in place. Network security requirements in this domain expresses the need for firewalls be put in place to support other security controls that supports identity and access management.

D5-Database Security: Requirements in this domain are expressed through the security controls implemented on logical storage containers such as object/file storage, databases or VHDs, where data is stored or archived on a digital storage location. The entire data security lifecycle incorporates two aspects of where the data is located and who has access to these storage location from the creation of data to its sharing or destruction. In the developed framework which will be presented in Chapter 5, it highlights the monitoring and encryption of data in transit at the Middle-Tier layer of PaaS and also on the Back-End of data at rest. Security controls and implementation that mitigate risks of data leakage, modification, vulnerable host operating system, virtual machines and hypervisors can be provided by cloud providers as components of the platform cloud. Data stored however must not be stored in clear text [86] but encrypted using industry standard cryptography techniques and encryption/decryption keys properly managed [87][88]. Authorized access to data stored on PaaS requires a secured channel via the API which is more or less highlighted in the network security and identity and access management implemented on this channel.

3.6 EXISTING APPROACHES

There have been an increasing number of studies and attempts in recent times to provide fundamental security management guidelines and techniques for assessing cloud computing security. These studies have offered various approaches in the area of security evaluation and assessment on PaaS and cloud computing in general. However, gaps have been identified which this research study fulfils in areas highlighted in the contributions to knowledge section of Chapter 1. This section discusses in detail, a critical analysis of existing related research studies, developed

frameworks and approaches in the area of security management and implementation of PaaS cloud architectures and cloud computing.

The Trusted Computer System Evaluation Criteria[89] developed in the U.S and issued in 1983, sets the basic requirements for assessing effectiveness of computer security controls implemented on computer systems. It was designed to evaluate security implementations in computer systems as well as to provide a standard to manufacturers as to what security features to build into their new and planned, commercial products in order to provide widely available systems that satisfy trust requirements (with particular emphasis on preventing the disclosure of data) for sensitive applications [89]. However an entity can only be classed as trustworthy if the parties or people involved in transactions with that entity rely on its credibility and trust in a cloud environment depends heavily on the selected deployment model, as governance of data and applications is outsourced and delegated out of the owner's strict control[90].

The CSA Cloud Controls Matrix (CCM) version 3.0 was designed for this purpose to provide a control framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains[49]. However, the CCM provides a more generic framework for all cloud services which recommends security controls to existing cloud delivery models and not specific controls for each individual model. Although the CCM is a good starting point and provides guidelines in ensuring security on cloud service models, it is not mapped to suit individual cloud service model architectures and not based on security requirements of cloud customers. The CCM does not provide a systematic way for cloud customers to evaluate cloud providers based on the security requirements identified by the customer.

The CSA through the CCM provides control specifications which emphasises business information security control requirements by combining existing industry standards to reduce security threats and vulnerabilities in the cloud. The Consensus Assessments Initiative Questionnaire v3.0.1 (CAIQ) on the other hand provides an exhaustive list of questions which customers can ask providers based on security offerings and implementation. However with the answered questions, cloud customers are faced with the tasks of evaluating the cloud architecture to ensure security provided by the provider is fit for purpose.

In a survey conducted by Subashini and Kavitha[91], a taxonomy presented which compared the similarities and differences between architectures of existing cloud service delivery models. Although few security controls implemented on different PaaS clouds were identified, the study did not describe what risks they mitigated. The study also did not provide in detail, security mechanisms implemented in the cloud and how they meet industry standard requirements.

In a study by Wu and Buyya[45] a detailed approach was provided for evaluating security and privacy in cloud computing by comparing security provisions offered by Amazon EC2, Windows Azure and Google App Engine. The study also attempts to answer security concerns raised by cloud customers who are curious to know what CSPs are doing to ensure security of their data in the cloud. Although, the study is useful for novice customers who are sceptical about cloud adoption and security, it does not provide security professionals with extensive details of the type of controls implemented to meet industry security attributes or requirements. The study also did not highlight security mechanism implemented within cloud components or demonstrate how they are integrated to meet specified security attributes. However, the research serves as a source of motivation and offers an initial strategy in the identification of security provisions offered by these CSPs.

In a study by Da Silva et al.[92], an approach was put forward for management of cloud computing security using the GQM (Goal-Question-Metric) methodology to develop a security metrics hierarchy to produce a security index as a criteria by which cloud security can be measured. This approach provides the avenue to evaluate security based on management priorities.

A developed framework was presented in the study by Kalloniatis et al.[93] to support selection of cloud providers based on security and privacy requirements. The framework provided a systematic and structured approach that enables software engineers to identify security and privacy requirements. Although the framework is useful for corporate cloud customers to identify their security requirements based on their organisational goals, it does not support individual customers and how their requirements can be identified. The study also does not address the evaluation process based on the identified requirements to understand risks in the selection of cloud providers. Customers will still require the use of an evaluation framework, depending on the cloud service architecture; to conduct a security risk assessment to ensure identified requirements are met by providers.

In Abbadi's cloud security and management study[21], emphasis was made on the analysis of cloud properties in an attempt to assess operational trust of services delivered by cloud service providers and ensure cloud customers make the right choice in the selection of IaaS CSPs. Although cloud properties listed as reliability, resilience and availability; which revolve around information security were identified; the security parameters and domains that govern these properties were not described. The study concluded the types and terms of SLAs can help determine cloud security assessments but did not develop a model or framework to conduct such assessments.

In a study by Nabeel et al.[77], a framework was proposed to evaluate trust on IaaS clouds. The framework presented a data gathering process of logs within the cloud service and the corresponding result can be used to determine the level of trust. However, the study did not discuss in detail, how trust is measured and how trust on IaaS clouds can vary depending on the security implementations configured on the cloud service.

In a study by Saripalli and Walters[94], a quantitative impact and risk assessment framework for cloud security was proposed. The framework proves useful in assessing and identifying the risk on cloud environments based on a scale of high, moderate and low; which can therefore be used to evaluate security implementations in such cloud environments. A new methodology for security evaluation in cloud computing was presented as an extension of the ISO 27001:2005 standard in an attempt to add more control objectives and make the standard robust.

Subashini and Kavitha[95] in their work suggested the development of a framework conceptualisation of the cloud security based on real world security system where it security depends on the requirement and asset value of an individual or Organisation. They concluded that the heterogeneous nature of cloud service models makes them dynamic and hence a dynamic approach on security should be considered. Therefore the strength in security is directly proportional to the value of the asset it guards on such clouds.

In a study by Probst et al.[96], an approach for security evaluation and analysis in cloud computing was proposed. The approach is focused on evaluation of access control policies within the cloud infrastructure as well as evaluation of intrusion detection and prevention systems implemented in the cloud.

In a study by Almorsy et al.[97], a tenant oriented security management architecture was presented which allows service providers to enable their tenants in defining, customising and enforcing their security requirements without having to go back to application developers for maintenance or security customisations. Their research study however is specific and relevant to SaaS cloud environments and security of already developed applications.

In a study by Zardari and Bahsoon[98], they presented an approach by using obstacles for systematically modelling, analysing and mitigating risks in cloud adoption. Although the approach proves effective in performing a match between customer service goals and features of a cloud service provider, they however concluded that the analysis of managing risks and mismatches is down to the judgement of the evaluation team. They also concluded that a requirement engineering framework is needed to help cloud users in elaborating and specifying user requirements and matching it to the cloud provider's features. They added that such dynamic selection of cloud with respect to user requirements is challenging to achieve.

3.7 SUMMARY

Security on Platform-as-a-Service cloud models involves the understanding of the security and management responsibilities shared by customers and cloud service providers. It also involves identifying different types of customers and service delivery models. In this chapter, a detailed discussion on the relevant operational security requirements using the Cloud Security Alliance (CSA) operational domain to categorise and identify security requirements specification relevant to individual customer needs in PaaS clouds.

Existing and related works that contributed to and motivated this study were also discussed as well as gaps in these studies were analysed in detail. These related research studies agree that for a cloud

to be trustworthy and secure, security requirements need to be assessed and evaluated against certain criteria to ensure they are fit for purpose. These requirements include requirements laid out by customers and adhered to be security provisions offered by CSPs. Although major input in the field provide baselines and guidelines for establishing security and trustworthiness in cloud computing, an approach for identifying and evaluating PaaS security implementations based on customer demands are yet to be developed. This is however due to the difficulties surrounding gathering and classification of requirements specific to customers and unique to different cloud service deployment and delivery models.

This research uses existing and related works in the field as a spring board to develop a framework that can be deployed to identify customer security requirements, classify them into categories of security levels and assess whether security provisions offered and implemented are able to meet the identified requirements.

Chapter 4 : RESEARCH APPROACH AND METHODOLOGIES

4.1 INTRODUCTION

The pragmatic approach to research for this study involves the use of mixed research methods to achieve the aims and objectives stated earlier in Chapter 1. The approach involves using the method which appears best suited to the research problem. Mixed methods research is an approach to inquiry involving collecting both quantitative and qualitative data, integrating the two forms of data, and using distinct designs that may involve philosophical assumptions and theoretical frameworks[99]. The research approach for this study constitutes a multiphase mixed methods design introduced using a research process cycle which is common in the fields of evaluation and program interventions. In this cycle, concurrent or sequential strategies are used in tandem to best achieve the aim of the study and highlight the original contributions to knowledge.

4.2 RESEARCH METHODS

4.2.1 PRIMARY RESEARCH

Evaluation Methodology

The security evaluation, testing, risk assessment, and protection profiling (PPs) of information systems are processes in which the evidence for assurance is analysed against criteria for security functionality and assurance level[100][101]. This method involves a process in which the evidence for assurance is identified, gathered, and analysed against criteria for security functionality and assurance level[101].

According to Systems Security Engineering Capability Maturity Model (SSE-CMM/ISO/IEC 21827)[102], security metrics are important indicators of how well security services are present in an information system and can be used to measure its security maturity level. This includes identifying security goals, assessing security posture and supporting security life cycle of the information system. In this research, the evaluation method involves development of a security evaluation framework made up of control specifications from IT industry security standards, security requirements for PaaS clouds and security parameters which serve as criteria for measuring security functionalities and assurance level of the cloud architecture. Therefore, the identified criteria forges a baseline for the use of the evaluation methodology in the assessment of security controls and implementations on PaaS cloud environments.

In the initial phase of the framework development, a critical evaluation and analysis of PaaS cloud architectures was conducted. This enabled the segregation of the cloud architecture into layers which enables the identification of components within the cloud architectures. The segregation into cloud layers as well as identification of components in each layer is termed a reference model for evaluating PaaS cloud architectures. Components of the framework that will be used to evaluate each layer of the cloud architecture are forged and will be discussed in detail in Chapter 5.

The second phase of the evaluation method involves the deployment of the developed framework to assess and evaluate security provisions and their implementations in PaaS cloud models based on scenarios. The deployment of the framework is aimed at the objective of testing the effectiveness of the framework in the evaluation process. Techniques that are considered for the evaluation methodology are described as follows;

a. Scenarios

To classify customer security requirements that are expected to be met by security implementations in PaaS cloud models, a set of scenarios is developed. These scenarios represent profiles for individual PaaS cloud models and includes their respective security requirements. The scenario comprises of a storyline describing the intended cloud service usage, service level objects, perceived threats and use pattern for the cloud model by the customer. They therefore create baselines for the customer's security requirements analysis.

b. Simulation

This technique involves the building of computer simulations and models that represent the actual system in order to perform experiments or tests.

Using this technique, the researcher intends to use findings from the evaluation and developed framework to set up a PaaS environment simulated on a single computer or distributed computer systems. Security mechanisms prevalent on existing PaaS cloud architectures will be implemented in this environment. This will create a test bed for the experimental approach to determine the effectiveness of the developed framework and how security mechanism implemented on the platform meet security requirements on PaaS private clouds.

c. Experiments (Testing and Assessment)

To find out how effectively the security framework meets the requirements and addresses security issues, it is necessary to perform an experiment on the simulation model already built. According to [16] "Since models are a description of reality, it is important to assess

these models and test their validity. In order to assess a model, the scientific methodology consists of making hypotheses and testing them through experiments".

The security mechanisms architecture in PaaS cloud models in the scenarios will be assessed based on security implemented in the simulation environment and tested for security vulnerabilities. This internal testing and assessment process will involve conducting series of vulnerability assessments and audits with the intention of verifying the capabilities of security implementations in the cloud models. It will involve the assessor adopting privilege access to the cloud models in order to conduct the assessment. In addition, a vulnerability log is produced which highlights layers and security domains within the cloud architecture where threats can be launched. The assessment and analysis will help determine how effective the framework is, in the evaluation of security in PaaS clouds based on security mechanisms implemented on each component of the cloud. Techniques that will be used in the security assessment and testing are categorised and described as follows:

- ***Manual Techniques***

In this study, the use of manual techniques for security testing and assessment by actively interacting with the PaaS Cloud models without the use of automated tools. These manual techniques include:

1. ***Privilege Elevation***- This involve the intentional elevation of an attacker's privileges to ensure how well the system can be compromised once authorised entry is gained into the system. It creates the avenue for the exploitation of vulnerabilities by the attacker.
2. ***URL Manipulation*** -URL manipulation is the process of manipulating the website URL query strings & capture of the important information by hackers. This happens when the application uses the HTTP GET method to pass information between the client and the server.

3. ***Reconnaissance*** - It also involves gathering information by observing how the security implementations are coordinated to perform security verifications, validations, authentications and authorisations in order to gain first-hand knowledge**.**
4. ***Security Examination-*** This involves the checking, inspecting, reviewing, observing, studying, or analysing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence on the security behaviour of a system. The security examination technique in this study involves exploiting privileged access to inspect, review, observe and study the extent to which an attacker which similar privileges would be able to access data and information resources in order to compromise security in the cloud.

- ***Automated Tools***

  This involves the use of automated tools to scan the system for compliance with host application usage and security policies and security vulnerabilities. A vulnerability assessment is an automated scan to determine basic flaws in a system. This can be either network or application vulnerability scanning, or a combination of both. The common factor here is that the scan is automated and generates a report of vulnerabilities or issues that may need to be addressed. It also involves the process of identifying live components and services that exist on those components in the PaaS cloud model. For the purpose of the testing methodology, we considered the use of various software applications which perform both reconnaissance and scanning.

  [1] Microsoft Baseline Security Analyser (MBSA) - This software tools enable checks for updates of the operating system, data access components (MDAC), MSXML (Microsoft XML Parser), .Net Framework and SQL Server. The tool enables information gathering through scans for insecure configuration settings. The tools will be used to scan security

configurations within the private cloud architecture and server infrastructure for possible vulnerabilities.

[2] Microsoft Baseline Configuration Analyser (MBCA) - This tool will help scan for issues within the private cloud architecture to maintain optimal system configuration and analyse against a predefined set of best practices and reporting results of the analyses. These analyses will be performed on the server that hosts the Windows Azure Pack. This enables the scan to be performed across all layers and components within the cloud architecture.

[3] Nessus Vulnerability Scanner

Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access. It is one of the most widely used application for vulnerability, configuration and compliance assessments. It supports a broad range of operating systems, databases, applications in physical, virtual and cloud infrastructures. It also supports non-credentialed, remote scans; credentialed, local scans for deeper, granular analysis of assets; and offline auditing on a network device's configuration. It consists of lightweight programs that collate vulnerability and compliance data and relays its findings as a report. Nessus also provides the ability to locally audit a specific machine for vulnerabilities, compliance specifications, content policy violations, and more [103].

In this study, Nessus will be deployed as part of the security assessment for private PaaS cloud environment to detect possible vulnerabilities and generate reports in the evaluation and assessment of security implementations in private PaaS cloud model.

4.2.2 SECONDARY RESEARCH

Grey Literature Survey

Grey literature is an important source of information. Though not scholarly, it is produced by researchers and practitioners in the field. It can often be produced more quickly, have greater flexibility, and be more detailed than other types of literature. The use of grey literature in this research enables the gathering of up to date information on security provisions and mechanisms published through technical reports and white papers by cloud service providers and cloud security analysts. It provides a valuable source of information on existing cloud architectures, security features, security mechanisms and configuration capabilities that surrounds PaaS cloud security requirements domain. Rather than conduct a primary research through questionnaires and surveys to find out security capabilities and limitations offered by certain cloud service provider in the scenarios, the use of grey literature allowed the collation of widely accepted and publicly available resources, considered to be valuable with little or no cost to acquire.

Documentation Review

This approach under secondary research requires the gathering of known industry security assessment documentation that discuss details of similar technologies and security implementations used in PaaS cloud environments. This includes established reports, templates, journals and articles that provide evidence to security reports and vulnerabilities in the security evaluation and assessment process. It also focuses on technical accuracy and completeness which include security policies, architectures, and requirements; standard operating procedures; system security plans and authorisation agreements; memoranda of understanding and agreement for system interconnections; and incident response plans [104].

4.3 SUMMARY

In summary, this chapter discusses the research methods that are relevant and applicable to the study. The primary research methods considered for this study enables proper resource gathering and support procedures necessary to conduct an evaluation. The use of various methods and techniques that constitute a thorough evaluation and assessment of the PaaS cloud architectures and security controls were clearly presented. The secondary research method provides adequate evidence from literature which helps in the gathering of information which would have been difficult to obtain using primary research methods.

Chapter 5 : FRAMEWORK DEVELOPMENT

5.1 INTRODUCTION

The chapter discusses the development of an adaptive security framework which has been designed to evaluate security controls and mechanisms implemented on each layer of the cloud model. A detailed description of each phase of the framework processes is discussed and presented in a table including security risks that affect each layer of the cloud architecture and how the framework can be adopted by PaaS cloud customer and security auditors to evaluate security mechanisms implemented on PaaS cloud models.

5.2 PAAS SECURITY MANAGEMENT PROCESS CYCLE

Similar to the **Plan-Do-Check-Act (PDCA)** Management Cycle or Deming Cycle in Information Security Management Systems (ISMS) is an iterative method for the control and continuous improvement of security processes and products. In this study, the PaaS security management cycle (Figure 5.1), describes specifically, the various phases of the information security management processes considered in the evaluation, assessment and review of security controls on PaaS cloud models.

The cycle is used to present a wider picture of how the research presented in this thesis contributes to existing knowledge and developments in the area of security assessment and management. As presented in figure 5.1, the PaaS security management cycle, developed as part of this work, aligns with the ISMS and consist of 8 processes that are required for the security requirements identification and management. The security framework presented in this chapter is designed to be used across 7 processes (2-8) in the cycle. Each process of the presented cycle is described in detail as follows.

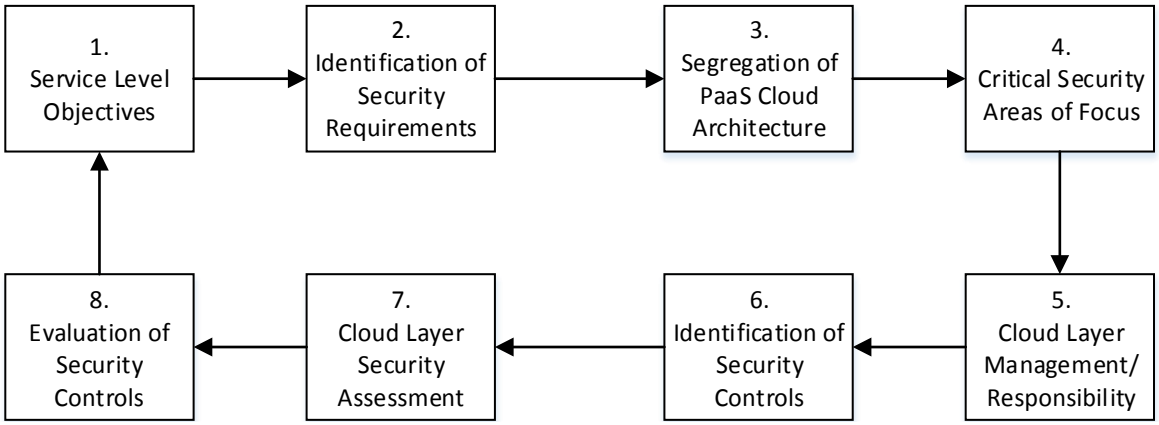

FIGURE 5.1: PAAS SECURITY MANAGEMENT CYCLE

[1] Service Level Objectives- In this process the generic service level objectives are identified by the cloud customer otherwise known as business requirements. It allows customers to describe several expectations and service level offerings expected to be delivered by the cloud service provider. This phase creates a typical scenario for security requirements amongst other functional and non-functional requirements a user may have. There are several factors that determine a customer's service level objectives. These include the value of the data assets, programming language of choice supported by the platform, uptime and downtime statistics, security risks and risk assessment, scalability, cost and return on investment.

[2] Identification of Security Requirements- This process allows the establishment of the scenario for the evaluation of the PaaS cloud model. PaaS cloud customers are expected to specify their desired security requirements using the security classification which describes the level of security controls and implementations. For each specified requirement, a scenario emerges and statistics generated which are used to determine the critical security areas of

focus as well as essential security requirements. An approach for identifying and classification of security requirements is presented in this study.

[3] Segregation of PaaS Cloud Architecture- During this process the PaaS cloud architecture is segregated into three: Front End, Middle Tier and Back End layers. The segregation enables us to identify components of the cloud architecture that provide different services and how the cloud infrastructure is integrated to support the environment. The segregation of the cloud architecture enables the identification of security areas within the cloud where controls and mechanisms are implemented for the purpose of security evaluation. A generic three layer architecture reference model has been developed in this study which can be used for various PaaS cloud service delivery and deployment models.

[4] Identifying Critical Security Areas of Focus- The identification and classification of security requirements and priorities enable customers to identify critical layers in the PaaS cloud architecture where security evaluation needs to be focused. Using a quantitative method of data gathering, customers can identify areas within the cloud architecture where their security requirements are prioritised as well as where security evaluation should be centred. A security mapping matrix, developed as part of this study has been designed to establish the critical areas within the cloud architecture where security requirements and provisions can be clearly identified.

[5] Cloud Layer Management /Responsibility- The objective of this process is to identify stakeholders responsible for the security management of a specific security area of focus or layer. This could either be the CSP or customer or both. The security mapping matrix presented in Chapter 6, clearly highlights stakeholders responsible for the security management in each layer of the PaaS cloud.

[6] Identification of Security Controls- The objective of this process is to identify the security controls implemented on the critical area of focus layers of the PaaS cloud architecture. It also relates to the security provision or capabilities that could be configured to enhance security on the critical area(s) of the PaaS cloud model. The security evaluation framework developed and deployed in this study enables the identification of security mechanisms and controls within security domains and architecture layers of the PaaS cloud.

[7] Cloud Layer Security Assessment - This process allows identification of security vulnerabilities or gaps that are not mitigated to an acceptable level after the evaluation of security controls and implementations phase. The objective of this phase is to determine if the risks of each layer of the cloud is reduced based on the security controls implemented of each layer or the security implementation capabilities it enables. A significant result of the analysis and assessment result will help determine the risk (High, Medium or Low) and vulnerabilities of each layer in the cloud service model.

[8] Evaluation of Security Controls- The objective of this process is to assess the identified security controls against the security requirements and classifications identified by the customer. This phase involves the assessment of the security features and offering of the cloud service considering the implementation of security controls and configuration to determine the security capabilities and limitations of the cloud service model. The process serves as the validation of security vulnerabilities found in an attempt to test the implemented security controls.

5.3 ANALYSIS OF PAAS CLOUD ARCHITECTURES

This section discusses the segregation of PaaS Cloud models and architecture into three distinct layers, which lead to development of the PaaS layers reference model. It further discusses the components of each layer and how they integrate to provide the service through its design and architecture. The most compelling challenge associated with distributed systems is the issue of security. Like all distributed systems which cloud computing is, the complexity of issues arises from the different points of vulnerability that exists in a distributed system[71]. The PaaS cloud architecture is made up of several components which consists of software tools and resources that are fully integrated as part of the development environment. This include physical resources, databases, services and system software over a distributed network accompanied with development languages and application frameworks. These components provide the building blocks for developers to create from simple websites to complex applications[105]. In order to consider it as a cloud computing offering, PaaS clouds must offer a way to create user interfaces, and thus support standards such as HTLM, JavaScript, or other rich media technologies[33].

Customers must be able to interact with the PaaS service model to enter and retrieve data, perform actions, get results and to the degree that the provider allows it, customise the service involved[33]. The PaaS should have built-in scalability of deployed applications including load balancing and failovers. It should also integrate with various web services and databases using common industry standards for flexibility. These components within the cloud architecture provide the service and experience for the customer in the development and deployment of applications.

Identifying how these components are stacked within the cloud architecture and how they integrate to provide secured communication of data in transit, data at rest and isolation of multi-tenant

customers' instances, provides the basis for the PaaS cloud model and the mitigation of security risks in the cloud. On the other hand, the identification of these components enable us to also pinpoint the security mechanisms and controls implemented on these integrated software tools and physical resources in the evaluation and assessment of information security on PaaS clouds. Figure 5.2 shows the PaaS cloud architecture segregated into layers. At the bottom of the stack is the platform physical resources that hosts the abstraction and operating system and network nodes. Access to this layer depends on the type of PaaS cloud model and responsibility of stakeholder managing the layer.

The segregation of PaaS cloud into three distinctive layers was done based on the functionality of the environment and the architecture of distributed systems of this nature. Although some CSPs may offer combined IaaS and PaaS or SaaS and IaaS cloud services on a single cloud service model, the segregation represented in our reference model consists of components and system functionalities that are centred to the provision of PaaS clouds only. A rigorous study of various existing PaaS cloud environments which include Windows Azure[106], Google App Engine[107] and OpenShift Origin[2] were conducted in order to understand PaaS cloud architecture (See Appendix A). The similarities in PaaS cloud architectures having components that include compute, storage and networking as the main service provisions that facilitates application development coupled with physical resources and application programming interfaces that allow these components to communicate, integrate and function seamlessly. It enabled the development and description of a three layer model that represents design and architecture of PaaS cloud environments.

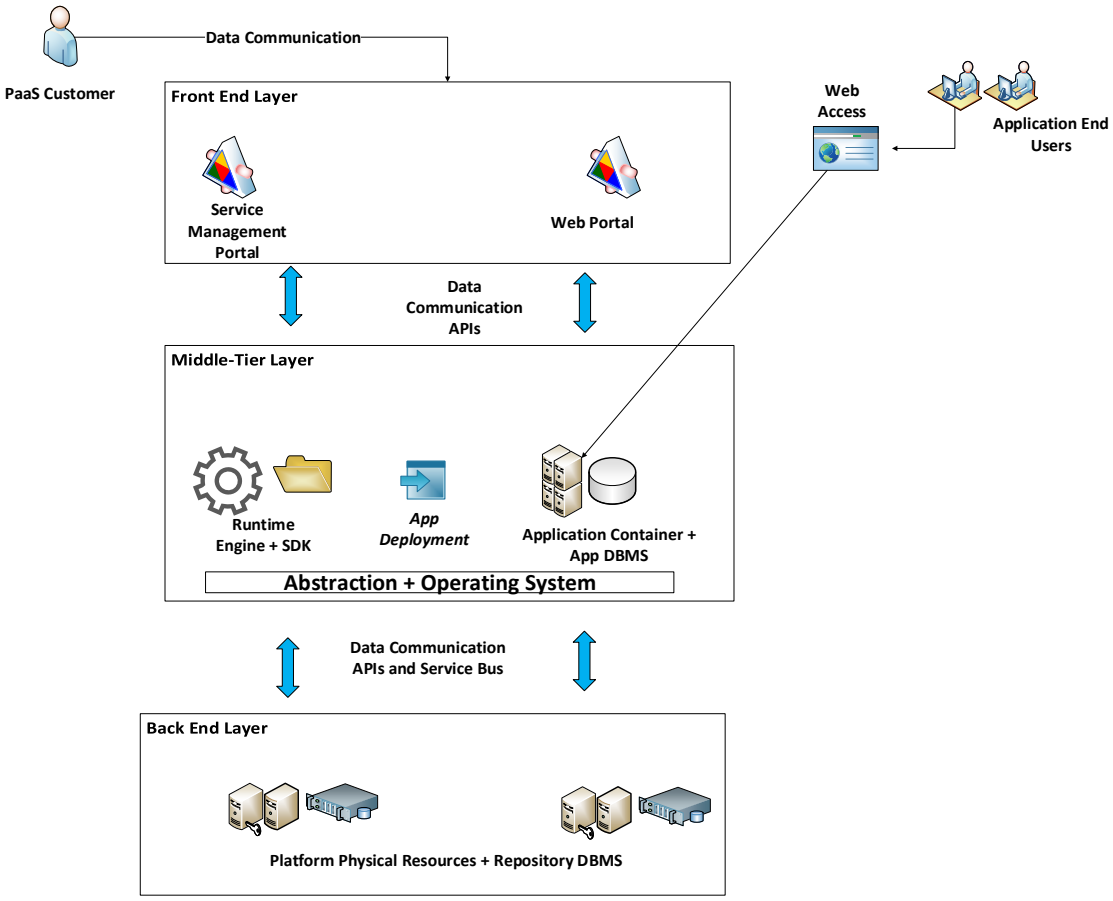

FIGURE 5.2: PAAS CLOUD LAYERS AND COMPONENT -REFERENCE MODEL

The remainder of this section provides a detailed description of each cloud layer and their respective components.

Layer 1 – Front End: This layer combines the developer user interface (UI) and service management portal. The Front-End presents the web services commonly known as the service- level. The interface consists of the application programming interface (API) which serves as the interface between the developer and the Platform-as-a-Service cloud environment. APIs present a user or developer with the platform to interact with the cloud service or have access to the cloud service to develop web based applications. It controls data flow and communication with the software and physical resources

depending on the provider and stakeholder management responsibility. The user is only able to access the PaaS using the API provided by the CSP or using an open standard API which is compatible with the PaaS as recommended by the service provider. Most APIs are web based and are implemented to support Representational State Transfer (REST) and or Simple Object Access Protocol (SOAP). The developer interface serves as the first line of entry to the abstraction layer for any user developing web based applications on PaaS. These APIs are designed to provide access and functionality for the platform cloud environment. This means integration with databases, messaging systems, portals, and even storage components[108].

The API comprises of software and applications libraries which enable it to interact with application development tools hosted on the Middle-Tier Layer. Software libraries made up of the service oriented-architecture (SOA) sits in between the API and OS to perform API calls which include service requests and response. The libraries ensure seamless integration of the various common and uncommon components of the PaaS cloud environment to interact with the front end user API and also with the Backend and logical storage databases of the platform. In Windows Azure for instance, the API is referred to as a Service Management API (SMAPI)[109]. Access to the PaaS storages or services is through the SMAPI over web services which enable customers to manage their data store and developed apps. On the other hand, customers can have access made through API programming command lines downloaded and installed via a Software Development Kit (SDK) such as Virtual Studio Web Express. A cloud service that provides just user management access through a web browser alone is regarded as a SaaS but alternatively through a command line API is a PaaS. The Front End layer in PaaS cloud architectures provide the avenue for the developer to ensure that

developed and deployed web based applications function correctly and are monitored on the platform.

Layer 2 – Middle-Tier: This layer sits in the middle of the stack, hence the name. It consists of the Abstraction (Virtualisation), Runtime Engine, Software Development Kit (SDK) and Operating System. The layer also hosts the application container and application database management system and communicates with the Front End and Back End layers through APIs or network communication channels allowed by the CSP. End users of developed applications have access through interfaces dedicated to applications and repository resources useful to the applications as shown in Figure 5.2. The runtime engine consist of modules that convert the programming language to machine language and services such as compiling, debugging, generation of source code and deployment of application to the application container. It interacts with other components on the platform by making API calls. Coupled with the Runtime Engine is the SDK. The SDK contains various executable files and software tools that invoke the runtime engine and enables the customer to develop applications based on the programming language. Both the Runtime Engine and SDK make up the runtime system or environment. In Windows Azure, this environment is known as the Development Fabric and on Google is referred to as the App Engine runtime environment.

The abstraction component provides a virtualised representation of the underlying hardware where the Middle-Tier layer sits. Abstraction invokes the physical resources such as processors, memory, disk and network capacities, combined with the operating system to create instances of the runtime environment for multiple customers. It also provides access to storage devices which are often replicated for redundancy[33].The pool of resources ranging for physical to storage resources are shared through load balancing which not only shields the customer from the service-based

architecture but also enables the PaaS delivery to be scaled in order to improve high availability and reduce service failover. In most PaaS cloud architectures, the Middle-Tier layer comprises of the computer, storage and network which are abstracted from the underlying hardware resources. These represent processing power to compile and execute software codes and libraries, store some sort of data on a repository and also connect several multi-tenant nodes through a network to resource pools of the underlying physical platform resources and dedicated nodes.

Layer 3 - Back End: This layer is made up of physical platform resources that hosts the PaaS architecture and network nodes. Depending on the type of PaaS service cloud model, platform physical resources could be in form of virtualised servers or bare metal servers that run within a distributed network. The layer also consists of a repository Database Management System (DBMS) that hosts the entire cloud data. The DBMS stores data for different customer accounts, profiles and instances of multi-tenant cloud customers which could be stored on either object/files storage, databases or virtual hard drives. Since the abstraction presents a logical representation of the Back End, the storage component of PaaS presents logical storage capacity for the backend data. For example, if a developer's application deployed in the cloud requires a backend data pool for resources to run correctly, the data can be stored on these logical storage allocations to serve this purpose. Certain virtual hard drives (VHDs) store guest OSes which enables the creation of virtual machines that run on the cloud platform. However, this is peculiar to PaaS clouds that support the creation of virtual machine instances as part of the cloud service solution offered by the vendor.

The hardware and network consists of the network nodes and disk allocation space on the physical machine or datacentre. This ensures that the right disk space is allocated during the creation of VMs and ensures that multi-cloud tenants can share resources from the same datacentre. This component also maintains failovers and availability of the cloud platform. Access to the Back End is done via

APIs, which enables a connection to be established from the Front End through the Middle-Tier. The repository DBMS can be accessed via a connection string through identification and access management parameters configured for authentication and authorisation of users.

5.4 PAAS SECURITY EVALUATION FRAMEWORK

The PaaS security evaluation framework was developed to be used in different phases of the security requirements identification and management process cycle. The framework is designed to provide a security mapping tool for cloud customers to assess the security implementations put in place to mitigate security risks on the cloud. It is aimed at providing a detailed template for understanding the security mechanisms, security methods, security threats and security requirements domain that enable security evaluation and assessment to be conducted on various PaaS cloud models once security requirements have been identified by the cloud customer. The overall architecture of the framework and its main components as shown in Figure 5.3 are described in details below:

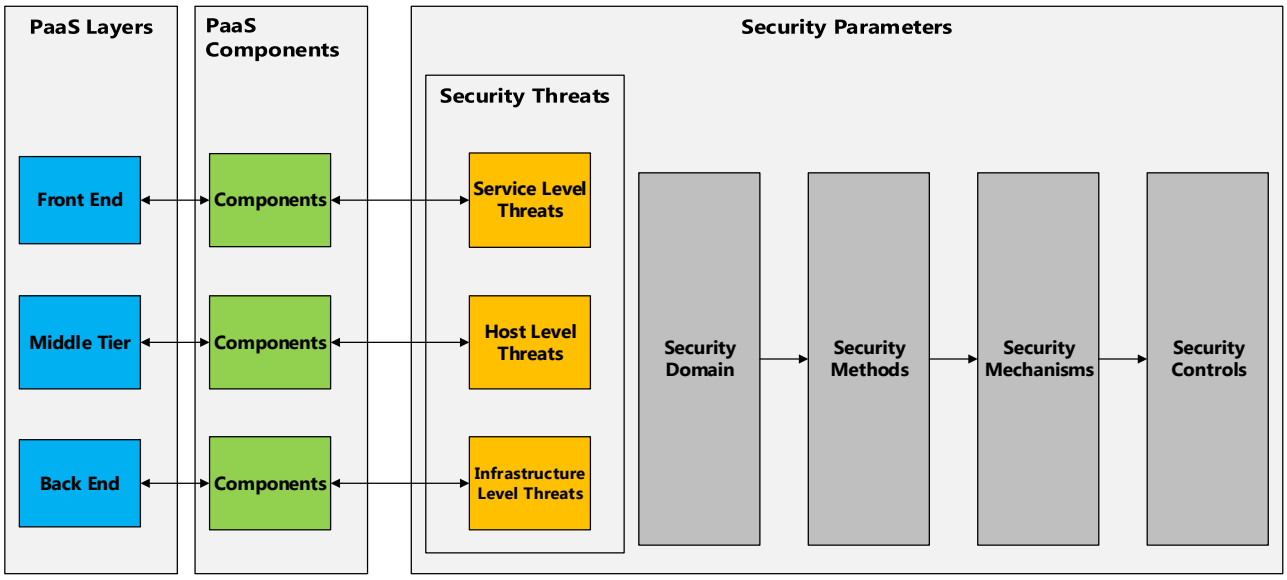

FIGURE 5.3: PAAS SECURITY EVALUATION FRAMEWORK ARCHITECTURE (OVERVIEW)

Security Parameters

These can be described as characteristics, features, or measurable factors that can help in defining the security provisions and offerings of a particular system. They are the measurable factors by which security provisions in the PaaS clouds are defined. The security parameters for the evaluation framework are defined as follows:

- **PaaS Components:** Components within each layer of the PaaS Cloud model.
- **Security Domains:** These are a list of security operational domains which focus on tactical security concerns and implementation within the cloud architecture as described by the CSA[49].
- **Security Threats:** List of events or actions that could cause loss of data or damage to the cloud environment. Threats exploit vulnerabilities within the cloud security architecture and sources of risks to the preservation of confidentiality, integrity and availability of components, resources and assets in the cloud. They are categorised into three types which are Service, Host and Infrastructure level threats discussed in Chapter 3.
- **Security Methods:** This describes the procedures or techniques that are used to secure the layer of cloud architecture from vulnerabilities, threats and risks.
- **Security Mechanisms:** It describes a group of security features and methods such as tools, protocols, applications or procedures for enforcing security policies in the PaaS cloud environment.
- **Security Controls:** Describes a type of security mechanism that provides security capabilities to meet a specific security requirement.

The framework architecture's foundations rest on industry best practices of identifying security domains that surround customer security requirements and tailoring these requirements into a security architecture framework. This enables customers to understand where specific security controls are being implemented within the cloud architecture. As an evaluation framework, it provides clarity and can be scaled to customer security requirements in an information security management system to access security compliance, capabilities and limitations in order to provide a gap analysis. The elements in each component of the framework are presented in Table 5.1 where security controls can be identified and completed into the table, once the security evaluation and analysis have been conducted. The framework consists of security parameters applicable to each cloud layer. These are presented in table in columns and rows. Each row closely matches with the PaaS three layers, while the seven columns highlight the security parameters that help define the security architecture of the PaaS cloud service deployment models. The detailed description of each component and layer is provided in Table 5.1.

TABLE 5.1: PAAS SECURITY EVALUATION FRAMEWORK

PaaS Layer	PaaS Component(s)	Security Threats	Security Domain	Security Methods	Security Mechanisms	Security Controls
Front End	Service Management Interface Web Portal	Service Level Threats	Identity and Access Management	Authentication/Authorization Methods Access Control Methods	Single Factor Authentication Multi-Factor Authentication Third Party Identity Authentication Role-Based/Mandatory Access Control	
			Encryption + Key Management	Encryption Method Session Management	Asymmetric/Symmetric Encryption Key Distribution	
			Network Security	Auditing/Logging	Static/Proxy Firewall Packet Filters Network IDS/IPS	

PaaS Layer	PaaS Component(s)	Security Threats	Security Domain	Security Methods	Security Mechanisms	Security Controls
Middle-Tier	App Container+ App DBMS Runtime Engine + SDK Abstraction +Operating System	Host Level Threats	Virtualisation Security	OS Patching Malware prevention/detection Auditing/Logging	Software Updates Anti-Malware	
			Network Security	Data Monitoring Auditing/Logging Sandboxing/ Multi-tenancy	Data Isolation Mechanism Host IPS/ IDS Packet Filtering	
			Database Security	Encryption Method Data Recovery Methods	Asymmetric/Symmetric Encryption Backups/ Failover	
			Encryption + Key Management	Encryption Method Session Management Key Distribution	Asymmetric/Symmetric Encryption Key Distribution	

PaaS Layer	PaaS Component(s)	Security Threats	Security Domain	Security Methods	Security Mechanisms	Security Controls
Back End	Platform Physical Resources + Repository DBMS	Infrastructure Level Threats	Database Security	Encryption Method Data Recovery Methods	Asymmetric/Symmetric Encryption Backups/ Failover	
			Identity and Access Management	Authentication/Authorization Methods Access Control Methods	Single Factor Authentication Multi-Factor Authentication Third Party Identity Authentication Role-Based/Mandatory Access Control	
			Network Security	Data Monitoring Auditing/Logging Sandboxing/ Multi-tenancy	Data Isolation Mechanism Network IPS/ IDS Packet Filtering	
			Encryption + Key Management	Encryption Method Key Distribution Data Recovery Methods Malware prevention/detection	Asymmetric/ Symmetric Encryption Custom Key Management Standard Key Management	

Note: In the Table above, the Security Controls column is blank. Security controls relevant to each cloud layer and component will be indicated in the column once security evaluation is completed. Customers intending to use the framework to evaluate security implementations in a PaaS cloud architecture would be required to complete the column with relevant controls found in reference to their security requirements as identified from their security evaluation of their chosen PaaS cloud model.

5.5 SUMMARY

Security evaluation and assessment is a process that has to be reviewed constantly to ensure the security controls implemented are fit for purpose in mitigating identified security vulnerabilities and threats. The Framework described in this chapter provides a granular detailed approach for security evaluation of security controls on PaaS cloud models. It provides cloud security analysts with a model which can be used to evaluate security solutions implemented in each layer of the PaaS cloud environment. The security parameters serve as components for the framework which allows specific security controls to be mapped with specific threats which are identified based on the methods and mechanisms used.

Chapter 6 : IDENTIFYING CRITICAL SECURITY AREAS OF FOCUS

6.1 INTRODUCTION

This chapter describes a systematic and adaptive approach in identifying critical security areas of focus within the PaaS cloud architecture. The chapter begins with an overview of layered security which is used to describe security levels based on classification of security objects such as security mechanism and features. The criteria used in the classification of security requirements in each security domain, is based on the multi-level security attributes of security mechanisms and features implemented to mitigate security threats and vulnerabilities. With the use of a security mapping matrix, customers are able to determine critical areas in PaaS cloud model architectures where their security implementations can be assessed, evaluated and reviewed. The security mapping matrix uses a quantitative method of analysis to gather security requirements classified as high, moderate or basic from the customers service level objectives to determine critical security areas of focus in the cloud architecture.

6.1.1 LAYERED SECURITY AND COMPLIANCE

The use of multi-layered security also known as defence in-depth, describes a defensive strategy featuring multiple defensive layers that are designed to slow down an attacker or intruder [110]. A holistic security approach should consist of multiple methods - user training, strengthened security policies and compliance screening, threat monitoring and targeted application protections, network and user access controls, encryption and system auditing, to protect against data loss[111].Therefore the security level of such holistic approach depends on the layer of security implemented and how strong the defence mechanism is.

It should be obvious that many common security mechanisms can be described as classifiers or have important aspects that fit into the framework of classification[112].With this approach in mind, security levels can be drafted based on the layers of security mechanisms implemented to provide security within security domains in PaaS clouds. The more rigid the security layers are, the higher the security level. On the other hand, these layered security must be compliant to industry models relevant to the data, assets and resources shared, stored or transmitted in the cloud. Examples of these compliance models include the PCI DSS, GBLA, FISMA, HIPAA and HITECH.

6.2 SECURITY LEVEL CLASSIFICATION

The classification of customer security requirements and security provisions implemented in PaaS clouds can be classified based on information security objectives and impact levels associated with information security, which affects the confidentiality and integrity of information should it be compromised[113]. Security requirements specifications and security provisions alike can be classified based on the potential impact to the preservation of security in the cloud. Table 6.1, shows the potential impact definitions for security objectives which includes confidentiality and integrity.

TABLE 6.1: POTENTIAL IMPACT DEFINITIONS FOR SECURITY OBJECTIVES [114]

	Potential Impact		
Security Objectives	**Low**	**Moderate**	**High**
Confidentiality	The unauthorised disclosure of information could be expected to have a limited adverse effect on organisational operations, organisational assets, or individuals.	The unauthorised disclosure of information could be expected to have a limited adverse effect on organisational operations, organisational assets, or individuals.	The unauthorised disclosure of information could be expected to have a severe or catastrophic adverse effect on organisational operations, organisational assets, or individuals.
Integrity	The unauthorised modification or destruction of information could be expected to have a limited adverse effect on organisational operations, organisational assets, or individuals.	The unauthorised modification or destruction of information could be expected to have a serious adverse effect on organisational operations, organisational assets, or individuals.	The unauthorised modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organisational operations, organisational assets, or individuals.
Availability	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organisational operations, organisational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organisational operations, organisational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organisational operations, organisational assets, or individuals.

In this section, security level classification is based on two areas:

[1] Customer Security Requirements that needs to be satisfied to achieve best security standards and practices on PaaS cloud models. They are security requirement specifications that are demanded by the cloud customer based on service level objectives expected to be met by the CSPs' security mechanisms and implementations in the cloud.

[2] CSPs' Security Provisions offered by CSPs by default, configuration or demand. These security provisions include security mechanisms and controls that are implemented to preserve the confidentiality, integrity and availability of customer data and resources and also secure the PaaS environment from being compromised.

The security requirements specification and security provision classifications are forged from security risks and potential impacts to assets stored and assessed on the cloud as well as other security and service level objectives identified by the customer. The security levels of each requirement and provision are described in detail and ranked into four unique classes which are High, Moderate, Basic and None. Each security level from High, Moderate, Low and None are assigned numeric values 3,2,1,0 respectively. The numeric values represent the security mechanism description for each classification based on the multiple layers of security features which meet requirements on each domain. PaaS cloud customers can therefore align security requirements they expect to be met by security features and controls implemented on the cloud architecture to reduce technical risks as described in ENISA report based on the estimation of risk levels on ISO/IEC 27005:2008 [94][43]. Each PaaS security classification is discussed in detail:

TABLE 6.2: SECURITY CLASSIFICATION SCALE

Classification	None	Basic	Moderate	High
Scale	0	1	2	3

High: This security level classification describes a multi-layer security mechanism to be put in place to protect the confidentiality, integrity and availability of sensitive data. The potential impact of security risks to data in this category is high from a risk assessment conducted by the cloud customer depending on the value of the assets in the cloud. Description for high security requirements comprises of customer's need for multiple layers of security mechanisms and controls that enhance security and also ensure that the system recovers quickly when under attack. It is suggested that having multiple complementary layers of protection defends against a broader range of threats and mitigates the risk of any single countermeasure being circumvented[115]. For instance in Identity and Access Management domain, a high security level classification requires that a security mechanism should consist of a strong authentication feature. An authentication which comprises of multi-factor authentication methods requiring two simultaneous but independent authentication methods commonly referred to as "something you have and something you know''[116]. The security mechanism must also consist of more than one implemented access control policy that governs who has access to certain layers or assets within the cloud architecture. For a customer requirement to be considered high, the multi-layered security description must satisfy detailed description shown in Table 6.3. It includes a combination of security best practices and a multi-level security architecture that suits security domain to ensure sensitive data is protected from security risks that could cause severe impacts on a layer(s) of the cloud architecture.

Adequate security controls can therefore be evaluated and reviewed to determine whether they meet the requirements set by the cloud customer for individual security requirement domain in a security audit process.

Moderate: This security level classification describes requirements for security mechanisms put in place to preserve the confidentiality, integrity and availability of data in transit and at rest on the

PaaS cloud environments where the value of data if compromised will result in moderate impact. However security implementations that meet this moderate requirements are considered as the minimum expected to be offered or provisioned to suit medium security risk impact. High level security controls that are fit to mitigate severe risk impacts, would be expected to meet a moderate requirement. A moderate security level classification also requires a multi-level security implementation to put in place on the cloud layer. However, the level is not as robust as a high security level and serves as a baseline between maximum security and minimum security implementations to ensure security on PaaS clouds. For example in secure data communication, a moderate security service would have HTTPS or TLS implemented between communication channels. However security services that include One-Time Passwords (OTP) or Tokens and Biometric authentication offers much stronger security and is considered a higher security service.

Basic: This security level classification describes security mechanisms put in place to preserve the confidentiality, integrity and availability of data in transit and at rest on PaaS clouds where the value of data if compromised, the impact is considered low or acceptable. A basic security level classification does not describe the non-existence of security mechanisms and controls standards, however it is considered as minimum security implementation and does not consist of multiple layers of security mechanisms implemented on the cloud layers stack. For instance, the provision of a password alone (single/ one-factor authentication) as the method of identification, authentication and authorisation will be considered as basic compared to a multi-factor authentication method when combined with other access management controls to form a strong identification and access management mechanism. As described in Table 6.3 below, basic security level classification describes having security implementations that provides at least a single layer of defence perceived to be required to mitigate low security risks.

None: This security level classification describes security mechanisms put in place to preserve no confidentiality, integrity and availability of data in transit or at rest. There are no baselines of security implementations in the criteria or description as risks are either non-existent or security controls are not applicable.

Once security requirements have been classified, adequate security controls implemented to meet such requirements can therefore be evaluated and reviewed to determine whether they meet the requirements set by the cloud customer for individual security domains in a security audit process.

TABLE. 6.3: SECURITY REQUIREMENTS CLASSIFICATION

Security Domain	Multi-Layered Security Mechanism Description	Security Level	Classification
D1- Identity and Access Management	Multi-Factor Authentication Mechanism: includes a Single Factor authentication +Second-Factor biometric authentication. Access control mechanism includes more than one Access Control Policy combined.	High	3
	Multi-factor authentication: Single Factor + Second-Factor Non-biometric authentication mechanism. At least one or more access control policy implemented.	Moderate	2
	Single Factor Authentication + Single or multiple access control policy.	Basic	1
	Security requirement not applicable or described.	None	0
D2- Encryption and Key Management	Endpoint to endpoint proprietary encryption with at least 256-bit PKI encryption key lengths. For instance, 256-bit (with ECDHE) or 2,048-bit (with RSA) for data in transit. Authentication and Key Exchange with at least 128-bits symmetric encryption. Certificate issued by Third Party CA. All data are stored in encrypted format/Hash using proprietary encryption mechanisms. (Data at Rest). Master or Key Encryption Keys are managed on a dedicated external host with restricted access control policies.	High	3
	Endpoint to endpoint Proprietary encryption with at least 192 -bit encryption keys (Data in Transit) Authentication and Key Exchange with at least 2048-bits encryption algorithm.	Moderate	2

	Certificate issued by Third Party CA. Master Key Encryption Keys are managed by an internally hosted key management system/solution.		
	Endpoint to endpoint proprietary encryption + at least 128-bit shared keys (Data in Transit). Authentication and Key Exchange with at least 1024-bits encryption algorithm. Certificate issued by Third Party CA. Master Key and Key Encryption Keys are managed locally with access control policies.	Basic	1
	Certificate issued locally and other Security requirements not applicable or described.	None	0
D3- Virtualisation Security	Host Intrusion Detection System+ Automatic Operating System patches and driver updates + In-built proxy firewalls. System log enabled.	High	3
	Host Intrusion Detection System + Stateful firewalls+ manual Operating System patches and driver updates. System log enabled.	Moderate	2
	Host Intrusion Detection System + static stateless packet-filter firewalls System log enabled.	Basic	1
	Security requirement not described or applicable.	None	0

D4- Network Security	Network is accessible over specific IP address pool/Virtual Private Network Remote Access to Network restricted. Proxy Firewall-Packet Filtering Mechanism implemented. Network Intrusion Detection System implemented.	High	3
	Network is accessible over a specified IP address pool/virtual private network Remote access restricted. Stateful-Firewall Packet filtering mechanism enabled. Network Intrusion Detection System	Moderate	2
	Network is accessible over public domain Remote access is restricted/permitted Static Stateless- Firewall Packet filtering enabled Network Intrusion Detection System	Basic	1
	Network is accessible over public IP address Remote Access permitted Packet filtering not specified or required.	None	0

D5- Database Security	Database allocated into schemas (Data at Rest) Database is encrypted using proprietary encryption. All data tables and columns are stored in encrypted format/ Hash using proprietary encryption mechanisms. (Data at Rest). Data store keys are issued dynamically and stored externally protected by a Master Key (Data at Rest)	High	3
	Database allocated into schemas (Data at Rest) All or Specific data tables and columns are stored in encrypted format/ Hash using proprietary encryption mechanisms. (Data at Rest) Data is encrypted using proprietary encryption. Data store keys are dynamically issued and stored within, protected by a Master Key (Data at Rest).	Moderate	2
	Database allocated into schemas (Data at Rest). All or specific data tables and columns are stored in encrypted format/ Hash using proprietary encryption mechanisms. (Data at Rest). Data is encrypted using proprietary encryption. Data Store keys stored within and protected by a password. Database password must be changed manually.	Basic	1
	Security requirement not described.	None	0

6.3 SECURITY MAPPING MATRIX

Mapping customer security requirements and CSP security provisions involves a method used to identify critical security areas of focus and prioritise customer security requirements within the PaaS cloud architecture. It requires matching and aligning identified security requirements into classifications of High, Moderate and Basic and then calculating the sum of identified requirements on each row in relation to the PaaS cloud layers. Likewise, security mechanisms provided and implemented by CSPs can be mapped. Mapping involves an operation that associates each element of a given set (the domain) with one or more elements of a second set (the range). To identify critical security areas within a PaaS cloud architecture, customers will have to manually feed their respective security requirement classification numeric value for each security requirement domain into each column and row of the customer requirements section in the matrix (Table 6.3). Each layer of the cloud is linked to management stakeholders as well as security requirements applicable on each layer. The summation of numeric values fed into the matrix is calculated; based on the summation of the values on each row which is described by the summative equation:

$$C = \sum_{i=1}^{5} Di$$

Where C is the sum of numeric values of each row in the matrix. The sum of each row implies:

Critical Area of Focus = $D_1 + D_2 + D_3 + D_4 + D_5$

Table 6.4 shows the security mapping matrix which consists of four sections on the top columns and four rows:

TABLE 6.4: SECURITY MAPPING MATRIX

PaaS Layers	Security Management Responsibility			Security Domain					Critical Area of Focus
	Managed	Semi-Managed	Unmanaged	Identity and Access Mgt.	Encryption+ Key Management	Virtualisation Security	Network Security	Database Security	
Front End	Provider	Provider	Customer	D_1	D_2	D_3	D_4	D_5	$\sum_{i=1}^{5} Di$
Middle-Tier	Customer/ Provider	Customer/ Provider	Customer	D_1	D_2	D_3	D_4	D_5	$\sum_{i=1}^{5} Di$
Back End	Provider	Customer	Customer	D_1	D_2	D_3	D_4	D_5	$\sum_{i=1}^{5} Di$
Prioritised Security Domain				$\sum_{i=1}^{3} Di$	$\sum_{i=1}^{3} Di$	$\sum_{i=1}^{3} Di$	$\sum_{i=1}^{3} Di$	$\sum_{i=1}^{3} Di$	

6.4 CUSTOMER SECURITY REQUIREMENTS PRIORITIES

PaaS cloud customers can choose security requirement classifications, described in Section 6.2, based on their service level objectives and potential impact to confidentiality, integrity and availability of computing resources and assets in the cloud. For each domain, security requirement values can be added to determine the domain with the highest value based on the mapping and identification of critical areas of focus. The domain with the highest value across the columns in the matrix table, highlights the security requirement with the highest priority to the customer. Hence the security mapping matrix does not only identify critical areas of security focus but also can be deployed to

determine the security requirement priorities based on the classification of security requirements entered and generated using the mapping matrix.

6.5 SUMMARY

This chapter presented a quantitative approach to identify critical security areas of focus or otherwise security requirements areas of interest within the cloud architecture. Based on customer requirements identified from the classification description and referenced using the scale, the mapping matrix enables customers to quantify their security requirements which can be compared to the security provisions offered by cloud service providers. The chapter also highlighted customer a method of identifying customer security priorities based on their requirements using a graphical representation of all security domain areas from the mapping result and analysis. Subsequent chapters in the thesis is focused on the security evaluation of PaaS cloud models and a presentation of analysis and results based on the evaluation findings. These will be based on the concepts presented in chapter 5 and this chapter.

Chapter 7 : FRAMEWORK DEPLOYMENT AND TESTING

7.1 INTRODUCTION

This chapter focuses on the deployment of the developed framework to evaluate two PaaS cloud models. The evaluation process as shown in Figure 7.1, involves the gathering of customer security requirement specifications and cloud provider's security offerings provisioned through the security mechanism and implementations in the cloud. These sets of data are classified using the security classification descriptions to generate two sets of data. The data sets are fed into the security mapping matrix individually to generate an output of the analysis which can be represented using a bar chart.

The output of the analysis of both sets of data are then compared to determine whether security provisions offered by the CSP meet the customer's security requirements. A security assessment is then conducted to determine which components within the cloud model architecture is vulnerable to security threats or attacks. With the use of scenarios to identify customer service level objectives and security requirements for each security requirement domain, this chapter is focused on demonstrating the effectiveness of the developed framework and mapping matrix in the evaluation and assessment of security controls implemented of layers of PaaS cloud models.

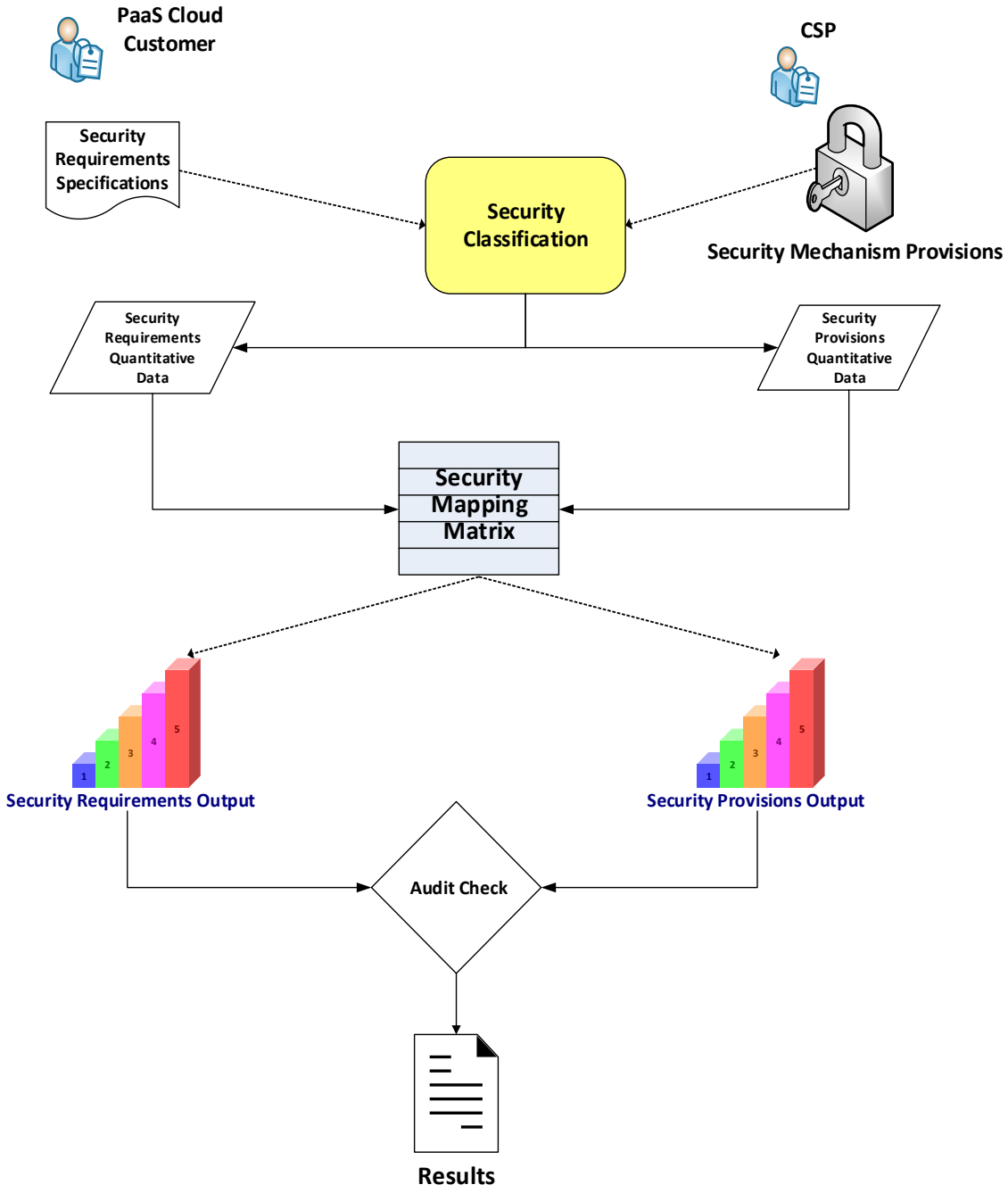

FIGURE 7.1: FRAMEWORK DEPLOYMENT PROCESSES

7.2 SCENARIOS

The evaluation methodology presented in Chapter 4, described the use of scenarios in the evaluation, testing and assessment of security implementations in PaaS cloud models. This section presents two scenarios with an overview of the security requirements for a Public (managed) PaaS and Private (unmanaged) PaaS clouds. Security requirements will be collated from the overview as well as security provisions offered in both clouds for evaluation and assessment using the techniques and methods from the proposed research approach and methodologies. The deployment of the framework, which has been conducted for the testing purposes for both scenarios is aligned with the PaaS security management cycle presented in Section 5.2.

7.2.1 SCENARIO 1

Managed Platform-as-a-Service Cloud

Bob is a lead IT security administrator and analyst for a start-up SME that intends to develop applications for their customer base in the UK. The SME wants to adopt a cloud service provider that complies with the industry standards such as ISO 27001/27002, SOC 1/SSAE 16/ISAE 3402 and SOC 2 and Cloud Security Alliance (CCM). Bob and his team are concerned about the security challenges and issues in PaaS cloud environments and have a security paperwork of requirements that they expect the CSP security implementations to meet. Bob considers choosing **Windows Azure**, a public (managed) PaaS cloud and is tasked with evaluating the cloud platform to determine if the service will meet the SME's service level objectives coupled with the SME's security requirements.

Security Requirements Mapping (PaaS Security Management Cycle: Process 2)

D1. Identity and Access Management- Identity service offered by the CSP should include or be compatible with multiple security authentications that allow customers to be authenticated and have access to the administrative management portal and backup servers. Security authentication should include multi-factor method of authentication and authorisation to provide additional checks and verification to the database repository, key repository or store and also retrieval of encryption keys. Access to sensitive components of the cloud architecture should be restricted to the role of the authorised customers.

D2. Encryption and Key Management- Security requirement provisions should include encryption of communication channels over a secure network. Additionally on the public network all communications between the cloud interface and end users of developed applications must be secure. The cloud systems should support only RSA 2048 keys or higher and provide customers the ability to generate keys which are stored on an attached standalone server (HSM), external to the platform cloud. Access to the HSM should be restricted to authorised customers with adequate role-based authentication and access control policy and backup initialised. The requirement also entails that the Organisation is in control of the key life cycle and can monitor key usage.

D3. Virtualisation Security- Operating systems should be hardened with regular automatic updates and a host-based logging audit that provides integrity of the files and software libraries. Proper secure boot technology must be integrated into the cloud platform to ensure that proper hardware and software modules are authenticated before they are executed within the platform.

D4. Network Security- Security service provided must provide or accommodate the creation of a segmented isolated network used for management and administration which is not accessible over

the public internet. The network security service should offer the capability for customers to create private networks for communication between components of the PaaS cloud. Each end user should be isolated on the network and prevented from interfering with each other. PaaS cloud should provide host-based network intrusion-detection tools (NIDS) or be compatible with open source NIDS; which have the capability of log analysis, file integrity checking, policy monitoring, and rootkit detection.

D5. Database Security- Security provision should include encryption options for storage and storage backups. The logs for the backup server must be monitored daily and be accessible to an authorised administrator. Cloud service should support the encryption of data volumes, databases and access to data should only be allowed through secure channels. Hardware Security Module (HSM) should be generate random security keys used to secure the data store and the server kept external from the cloud platform.

Security Requirements Analysis

With the use of the classification matrix, the customer's security requirements are analysed and classified into the description categories of High, Moderate, Basic and None. The security requirement mapping framework is then used to identify critical security areas of focus in the PaaS cloud architecture. A bar chart of the security requirements analysis is then generated showing the critical area of focus using the mapping matrix.

TABLE 7.1: SCENARIO 1- SECURITY REQUIREMENTS CLASSIFICATION

Security Domain	Security Mechanism Description	Security Level	Classification
D1. Identity and Access Management	Multi-factor authentication: Single Factor + Second-Factor Non-biometric authentication mechanism. At least one or more access control policy implemented	Moderate	2
D2. Encryption and Key Management	Endpoint to endpoint Proprietary encryption with at least 192 -bit encryption keys (Data in Transit) Authentication and Key Exchange with at least 2048-bits encryption algorithm. Certificate issued by Third Party CA. Master Key Encryption Keys are managed by an internally hosted key management system/solution.	Moderate	2
D3. Virtualisation Security	Host Intrusion Detection System patches and driver updates + In-built proxy firewalls. System log enabled. + Automatic Operating System	High	3
D4. Network Security	Network is accessible over a specified IP address pool/virtual private network Remote access restricted. Stateful-Firewall Packet filtering mechanism enabled. Network Intrusion Detection System	Moderate	2
D5. Database Security	Database allocated into schemas (Data at Rest) Database is encrypted using proprietary encryption. All data tables and columns are stored in encrypted format/ Hash using proprietary encryption mechanisms. (Data at Rest). Data store keys are issued dynamically and stored externally protected by a Master Key (Data at Rest)	High	3

TABLE 7.2: CRITICAL SECURITY AREA OF FOCUS ANALYSIS (REQUIREMENTS SPECIFICATIONS)

PaaS Layers	Security Management Responsibility			Security Domain					Critical Area of Focus
	Managed	Semi-Managed	Unmanaged	Identity and Access Mgt.	Encryption +Key Management	Virtualisation Security	Network Security	Database Security	
Front End	Provider	Provider	Customer	2	2	0	3	0	7
Middle-Tier	Customer/ Provider	Customer/ Provider	Customer	0	2	3	3	2	10
Back End	Provider	Customer	Customer	2	2	0	3	2	9
Prioritised Security Domain				4	6	3	9	4	

The data from the security mapping matrix can be represented with a bar chart to highlight critical areas of focus in the PaaS cloud. As in Figure 7.2 below, security requirement specification for each security domain are clearly shown with the critical area of focus highlighted in the graph. The graph indicates the Middle-Tier layer with frequency of 10 as the critical area where security requirements are more prevalent with network security requirements with frequency of 9, being the prioritised requirement across all domains.

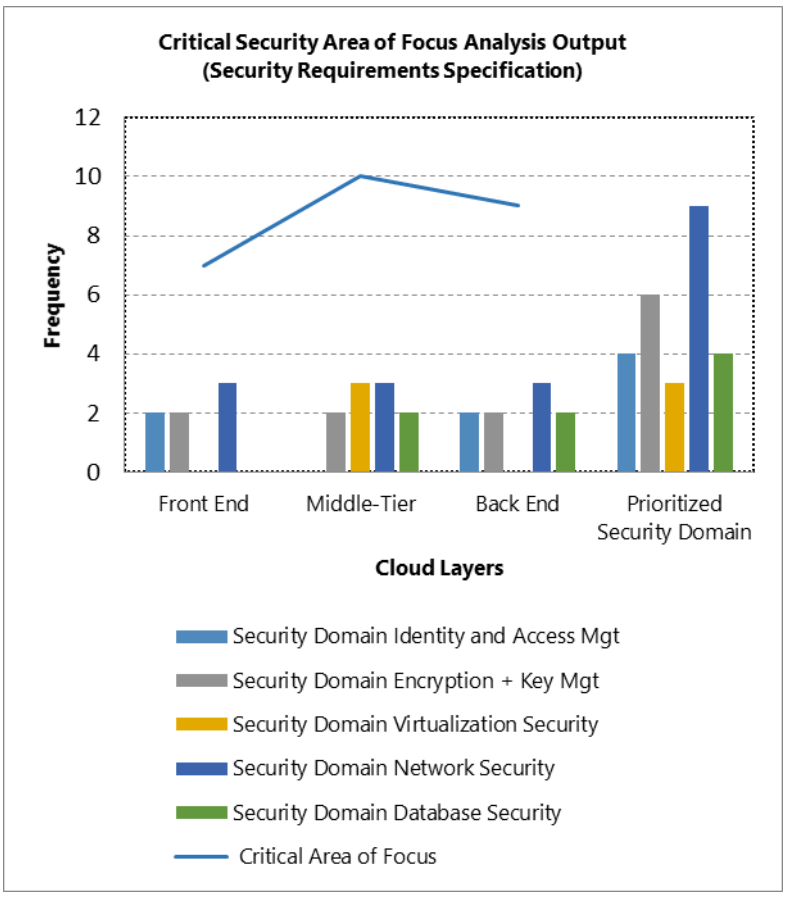

FIGURE 7.2: SCENARIO 1- CRITICAL AREA OF SECURITY OF FOCUS BAR CHART (REQUIREMENTS SPECIFICATIONS OUTPUT)

Segregation of Windows Azure PaaS Architecture (PaaS Security Management Cycle: Process 3)

The Windows Azure Platform is Microsoft's cloud platform that combines Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) offerings that runs on servers and related network infrastructure located in Microsoft data centres and is connected to the public internet[117]. According to Microsoft[118], Windows Azure is a combination of managed and unmanaged services that allows cloud customers build, deploy and manage applications. The architecture of Windows Azure was considered from existing literature and documentation provided publicly by Microsoft in their Windows Azure security overview[106]. The architecture consists of three major components that

facilitate the service amongst others and are placed on different layers of the PaaS cloud environment. These are network, compute and storage. The network provides the underlying infrastructure with the resources to connect with the PaaS environment while the compute component provides the platform for the provisioning of virtual machines (VMs) and the development of logic apps and web apps development before being deployed for hosting on the public internet domain. The storage component however provides backend storage resources for developed apps within the PaaS cloud as well as storage of VM instances and customer subscriptions on Microsoft data centres. Access to these components are made possible via interfaces and RESTful services which form part of the networking component described earlier and managed by the application and fabric services (AppFabric Services).

Segregating the Windows Azure PaaS architecture into layers, enables the identification of critical security areas of focus as well as mapping security requirements domain to components of the cloud where security implementations are being offered. From our initial analysis of PaaS cloud architectures described in Chapter 5, we considered the architecture presented in Kaufman[106]. However since 2010, the architecture of Windows Azure has evolved as all cloud environments due to their dynamic nature and more documentations have discussed components within the cloud architecture.

Layer 1- Front End: The initial point of entry for Azure developer and IT administrators to the cloud service is the Windows Azure Development Portal[117]. Currently known as the Azure management portal, it is a web based interface for managing the cloud platform. It has a dashboard that gives an overview of the cloud environment where developers can develop and deploy logic applications from templates provided through the CSPs template gallery. The portal, provides an avenue for

administrators and developers alike, to manage the health of developed and deployed applications, manage their subscriptions, configure security provisions, integrate their existing platform with an on-premises cloud, manage data analytics and review subscription billing.

The portal requires the customer to have a Windows Live account from which they can subscribe for a plan to access services provisioned according to the plan offered by Microsoft. This portal can also be accessed through a standard web browser or via a command line interface known as the Service Management Application Programming Interface (SMAPI)/ Azure PowerShell command line .The web browser UI consists of navigation frameworks and data management APIs. Monitoring of application data traffic and the performance of the environment can be done through the portal. The SMAPI allows for API calls to be made from the Software Development Kit (SDK) once applications are deployed or published; they can be viewed via the web portal or the source code previewed via the SMAPI.

Layer 2- Middle-Tier: In Windows Azure, the middle-tier layer is made up of the hosted service, storage service and the runtime environment that offers application source code execution and runs application services. Through the management portal, certain applications can use either the hosting or storage accounts or both. The accounts enable developers to host and deploy applications on the Windows Azure platform[119]. This layer offers the compute service; where developers can create VM instances, Websites from templates as well as other cloud services. VM instances are served by OS Virtual Hard Disks and Data Virtual Hard Disks supported by the underlying platform resources or Microsoft data centres. These are the IaaS capabilities and offerings offered on Windows Azure. To focus on the PaaS side, Windows Azure supports application development which are managed by automated cloud services such as worker and web roles. The web role is provisioned for web

applications and supported by Internet Information Service (IIS) while the worker role supports underlying features of the web role. Coupled with these cloud services is the developer tools and services. These include Visual Studio and Azure SDKs. Microsoft currently provides language-specific SDKs for .NET, Java, PHP, Node.js, Ruby, Python and C++. They serve as application development building blocks which developers use to build applications in the cloud which are deployed and hosted on applications containers known as PaaS VMs. On the other end of the Middle-Tier Layer is the Storage services of Windows Azure. It consists of object/files storage, databases and virtual hard drives known as Azure Blobs, Azure Tables, Azure Queues and Azure XDrives. These logical storages serve as backend databases for applications which can only be accessed via RESTful AP or HTTP calls. However the XDrives are VHDs created for the purpose of running VM instances on allocated storage drive spaces. The logical storages coupled with their application resources both reside in a container, known as the app container. Application end users have access to the application and applications can make calls to respective logical storages via Restful APIs or HTTP calls.

The underlying infrastructure that supports the compute and storage services of the Windows Azure platform is the **Abstraction and Operating System**. They are referred to within the architecture as **Windows Azure App Fabric and App Fabric Services**. Managed by the Azure **Fabric Controller** functions as the kernel of the Azure operating system, this capability is handled by providing a scale-out feature within the platform to manage a sudden increase in the volume of users accessing the system[119]. Coupled with the App Fabric Services, the Fabric Controller performs virtual tailored networking operations that link the tables, queues and blob storages with the hypervisor and the cloud core infrastructure components. It performs load balancing to manage failovers of the multi-

tenant customers sharing resources over the underlying resource pool. The App Fabric is the Abstraction and Operating System of Windows Azure coupled into one.

Layer 3- Back-End: This physical platform resources and database management system (DBMS) on Windows Azure is represented by **Microsoft servers and SQL Azure Databases**. Although these resources are hosted on physical servers on remote datacentres, they are however presented to the customer virtually via logical servers in geographic locations known as regions and accessed via the Front-End Layer. Customers can create or provision SQL databases and VMs which will live on these logical servers and deployment applications to be hosted on VMs and that have data access to the underlying SQL Azure databases from within the cloud environment or outside.

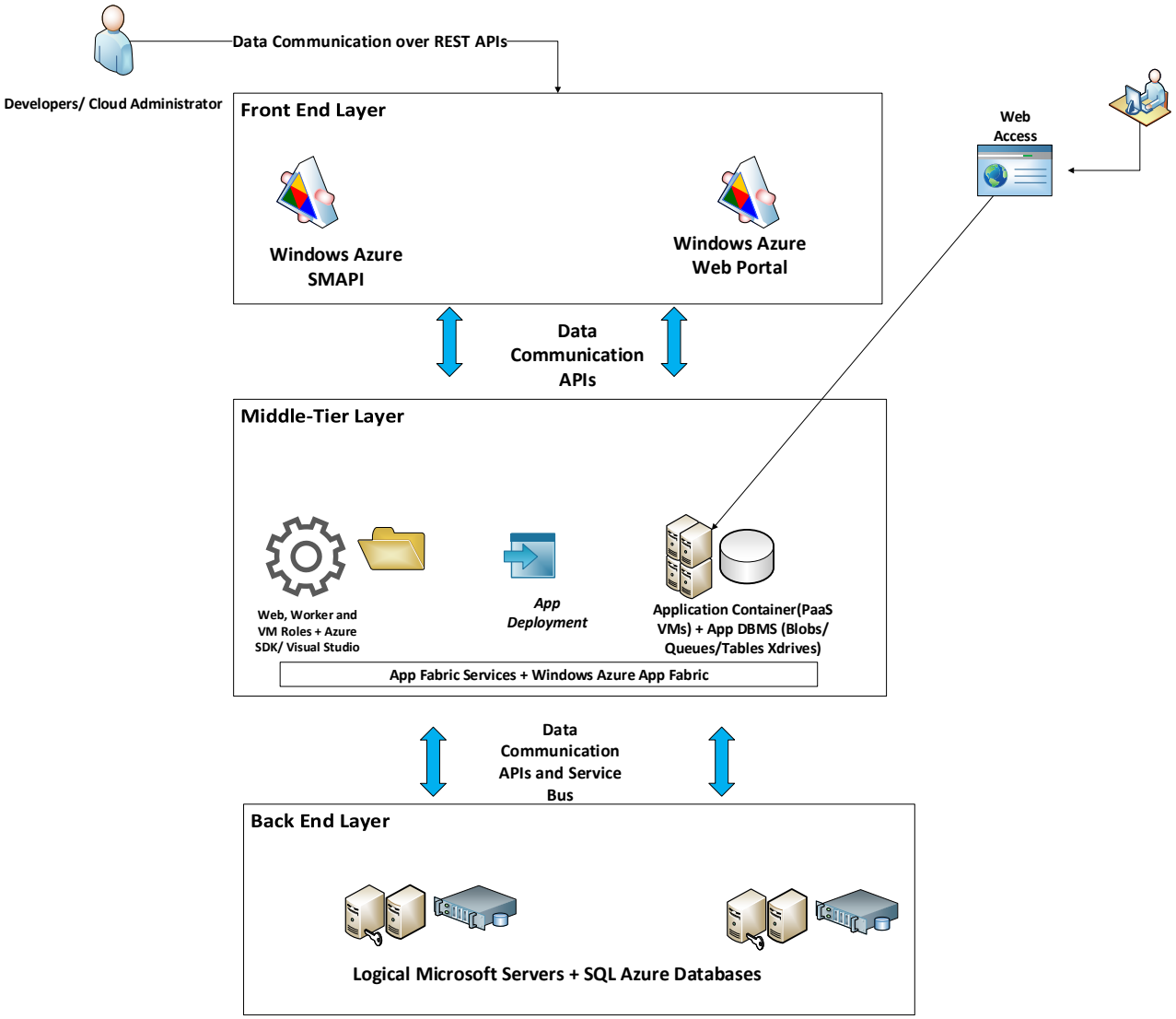

FIGURE 7.3: WINDOWS AZURE PAAS ARCHITECTURE AND COMPONENTS (REFERENCE MODEL ILLUSTRATION)

Security Evaluation of Windows Azure (PaaS Security Management Cycle: Process 4, 5, 6)

D1. Identity and Access Management

- **Single Factor Authentication**- Customers or IT administrators of this environment only require a Microsoft account formerly known as Windows Live ID to register to log in to the cloud service and register for a service subscription. The subscription account is setup with an email address and password with a credit card and mobile number as proof of identity.

These credentials are then sent to a Microsoft authentication server to be authenticated and verified using OAuth 2.0 tokens and Windows Identity Foundation (WIF) as customers only need the Microsoft Account email address and password to log in each time into the service subscription account. This feature is provided by default as having a Microsoft account enables Single Sign On (SSO) as Microsoft serves as the identity provider (IdP) for authenticating and validating user credentials.

- **Multi-Factor Authentication**- Window Azure provides comprehensive identity and access management solution by enabling administrators to implement multi-factor authentication (MFA) to authenticate users using security features provided at the Front End dashboard. MFA requires the use of more than one authentication and authorisation method to verify users. Alternatively, administrators can setup MFA to verify access to organisation cloud data and application resources. Moreover, MFA service can be implemented in Azure Active Directory to give users access to custom or on-premises applications. Administrators would have to manage MFA service on Windows Azure using an organisational credential and not Microsoft account. According to Kaufman[120], every administrative account of a Windows Azure subscription can get additional protection by enabling this core multi-factor authentication functionality. So an administrator that wants to access Azure portal to create a VM, a web site, manage storage, mobile services or any other Azure Service can add multi-factor authentication to his administrator account.

  Authentication Options Available of Windows Azure include the use of Multi-Factor Authentication (MFA) apps which are (Notification and One Time Passwords (OTP), Automated Phone calls and Text messages. These options involve the use of a mobile device, for instance a phone which is registered to the user's account, and serves as the second factor

authenticator. Once MFA is implemented, a customer or administrator would have to provide a Multi-Factor authentication consisting basically two methods of authentication:

- Single Factor- Something they know; typically a password.
- Second Factor- Something they have; a device such as a mobile phone or tablet

a) **Notification option**- For the notification MFA to be configured, the customer or administrator would have to download a MFA app on the registered mobile device. Once the administrator provides the single factor through the Front End layer on Windows Azure, a dedicated Microsoft authentication server sends a push notification to the administrator's mobile device upon the first stage of authentication which is the provision of a typical password in this case during sign in. The administrator receives the push notification on the mobile device and is prompted to either accept or deny the notification. On acceptance, the administrator is authenticated at the Front End.

b) **One Time Password (OTP) and Text Messages option:** In this instance, provision of the single factor (password) upon sign in, the MFA app serves as a software token and generates a passcode which is displayed to the administrator. The administrator then provides the passcode at the Front End as verification using a second factor mobile device for authentication. Invariably, the text messages function just like the OTP. In this case, the administrator is sent a text message to the registered mobile phone with a passcode. He then provides this second factor at the Front End to verify authorisation and authentication is completed.

The OTP uses the hash chain algorithm [121]: $h\,(h^{x-1}(p)) = h^{x}(p)$

Where (p) is password supplied by user and is hashed (h) of a finite digit (x) and stored on the server as h^{x}(p). For authentication, the user supplies password (p) which is hashed again

as (h^{x-1}(p)). The authentication server computes the initial stored hash with the new hash to produce a match where h (h^{x-1}(p)) = h^{x}(p) and the user is authenticated. This cycle is repeated for every hash value of (p) provided for a match with the initial hash value of (h^{x-1}(p)) stored by the authentication server during successful logins.

c) **Automated Phone Calls:** This MFA presents a mode of authentication by using a phone call as the second factor to verify and authenticate authorised users. The user or administrator receives a phone call and is prompted to press a digit on the phone keypad for authentication. The authentication mechanism requires a series of steps:

1. The user provides his Windows Live ID credentials as a single factor authentication via the Front End.
2. Front End verifies credentials against stored hash value and redirects user to place authentication call to the user's registered phone number setup by the administrator.
3. The call is placed through and the user is prompted to enter a specific digit from the phone keypad.
4. The digit is verified by comparing the stored hash value of the digit initiated by the authentication server with the one placed through by the user.
5. Upon authentication success, user is redirected to the Front End management dashboard.

- **Active Directory Federation Service (ADFS)** -Access Control policies at the Front End layer on Windows Azure is governed by roles and policies implemented when administrators configure Active Directory Federation Service (ADFS) on Windows Azure to manage access control restrictions. This ADFS is similar to an on-premises ADFS but service is hosted in the

cloud and not on-site. The ADFS allows administrators of the Windows Azure account to authenticate both additional internal admin accounts and end user accounts using the ADFS hosted on Microsoft Datacentres.

D2. Encryption and Key Management

- **Asymmetric Encryption**-Windows Azure [120] stores certificates and private keys in the PKCS12 (PFX) file format uploaded through its Front End. The PKCS12 is Public-Key Cryptography Standards (PKCS), published by RSA Laboratories, which defines a file format commonly used to store X.509 private keys with accompanying public key certificates, protected with a password-based symmetric key. The communication from the Front End to the certificate store is encrypted over SSL channels giving administrator privileges to upload and not download private keys at any time. The private keys and certificates are used by the Fabric Controller to initiate roles especially when deployments or application containers (PaaS VMs) are created by the administrator registered to a specific subscription.
- **Key Distribution**- These certificates and private keys used by the PaaS VMs are kept in the certificate store or key vault. Windows Azure provides a Key Vault which is an internal Hardware Security Module (HSM) for secure key management and storage of cryptographic keys and passwords. However for the PaaS VMs or applications to have access to database resources as well as storage resources, administrators would have to provide access to the key vault (HSM). The key vault provides SQL Server encryption to leverage the Azure Key Vault service as an Extensible Key Management (EKM) provider to protect its encryption keys. These keys are then passed on to applications that require the resources. Moreover, security of communication channels with application containers (PaaS VMs) and within the VMs are

protected with SSL and mutual authentication[59]. Windows Azure provides access to industry cryptography functionalities such as MD5 and SHA and encryption standards such as AES. These standards are provided by the .NET Cryptographic Service Provider (CSP) provided in Windows Azure.

- **Transparent Data Encryption (TDE) -**Data and resources stored at rest at the Back End (SQL Azure Databases) can be encrypted using the Transparent Data Encryption (TDE) which is used to encrypt an entire database using AES-256 symmetric key. The key is protected by a built-in certificate and kept in the Azure Vault which is rotated by Microsoft (CSP) every 90 days.
- **Column Level and Back up Encryption**- Windows Azure provides column level and back up encryption for the Azure SQL databases on different fronts. With the use of symmetric key encryptions such as AES 128, AES 192, AES 256, and Triple DES, information in each data column of the database is encrypted. It also ensures that the backed up data or entire database can be encrypted using any of the symmetric key algorithms for backup and retrieval decryption. These keys are stored with the key vault.

D3. Virtualisation Security - In Windows Azure, virtualisation security is provided on different fronts and closely integrated with network security. They include VM security, Abstraction security and OS hardening. PaaS VM security and isolation is provided by App Fabric Services and Windows Azure App Fabric while the IaaS VMs are isolated by the computer host which serves as a Hypervisor, coupled with the network functionality of the FC.

- **Virtual Appliances**- The use of virtual appliances such as web application firewalls (WAFs) to prevent cross-site scripting (XSS) and injections. The web application firewall prevents attacks

to the application container (PaaS VMs) where user applications and stored. Hence preventing a VM within the Middle-Tier from being compromised which can be used to instigate attacks to other VMs within the cloud architecture. However this security service is not provisioned by the default and would require the administrator to implement third party WAFs and integrate it within the cloud architecture.

- **Third Party Virtualisation Security**- In our evaluation, we considered the use of Barracuda Web Application Firewalls (WAFs)[122] which can be used to protect applications developed and deployed on Windows Azure once networking security configurations have been implemented to protect the PaaS web roles. The third-party WAFs can be integrated seamlessly to inspect network traffic serving as an intrusion detection and prevention system (IDS/IPS). What is provided by default is the restriction of inbound traffic from the Internet on a VM created through the Front End with the exception of ports used for remote management.
- **Microsoft Antimalware**- This antimalware agent can be enabled by the administrator in the Middle-Tier layer to offer protection to runtime environment which includes the Web role, Worker role, VM role and VMs. The antimalware can be scheduled to run to monitor the health of the cloud layer and collate events logs. The antimalware can be deployed via the SMAPI, using the SDK such as visual studio or via the PowerShell command prompt.

D4. Network Security-

- **Virtual Private Networks (VPNs)** - the abstraction which consists of the App Fabric Services and Windows Azure Fabric coupled with the functionalities of the FC. This abstraction layer is restricted to only accept inbound requests through dedicated IP subnets with an exception

to internet IP address or customer VMs. This thus prevents the abstraction from being compromised at any point. Moreover, coupled with virtualisation security discussed above, administrators can configure virtual private networks (VPN) to isolate communication and restrict communication between VMs. At the Back End, communication to the Logical Servers are restricted to the public internet and separation of various customer accounts and subscriptions (multi-tenants) using private networks. Communication between the Middle-Tier and the Back End Layers are cryptographically protected through secure SSL channels which allows administrators secure access to logical storage locations such as the Azure SQL repository DBMS.

- **Network Access Control Lists**- Like firewalls, Windows Azure implements Network ACLs to provide logical isolation of the customers' cloud environment. This enables the communication between VMs within a private network hosted in the cloud. The ACLs permit communication between endpoints or IP addresses only specified by the administrator. This mechanism is also deployed to provide isolated communication between multiple subscriptions of an individual cloud customer.
- **Built-in Firewalls (Windows Firewall)** - Windows Azure provides two sets of firewalls which have to be configured by the administrator to enable communication to the SQL databases. By default, all communications are blocked. The administrator can either specify firewall rules at the server or database level. The server level rule allows cloud tenants access to the entire logical database server while the database level govern rules which allow cloud tenants to individual databases within the administrator's Azure SQL Database server.
- **Network Security Groups**- Cloud customers or administrators can deploy network security groups within Azure as part of the security implementation provisioned by the CSP. This helps

to control traffic to specific VMs hosted in the Middle-Tier Layer of the cloud architecture. It acts like a filter for inbound and outbound network traffic which can be implemented on an entire subnet of VMs. The rules of a network security group must be enforced on the source and destination IP addresses as well as the port and protocol used.

- **Azure ExpressRoute**- Windows Azure provides Azure ExpressRoute sure as a security functionality that ensures security communications between the Microsoft Datacentre and customer on-premises datacentre. Typical for a hybrid or semi-managed PaaS cloud environment, the ExpressRoute uses communication channels provided by two types of providers to connect the on-premises datacentre with Microsoft's datacentre. These communications is achieved using point-to-point Ethernet links or VPN connection.

D5. Database Security

- **Shared Access Signature Token**- As mentioned in the identity and access management provisions offered on Windows Azure, Data Store security is a supported security mechanism to protect data stored in the Back End repository storage accounts. Storage accounts provide access to data stores such as DBMS repositories (Tables, Blobs, and Queues) and SQL Azure; are protected by a security mechanism called a Shared Access Signature Token (SAS). This token is generated by a pair of 512 bits Storage Access Keys which secure the storage account. The token is simply used for authentication requests when calls are made from a service or application that requires access to the storage as an attachment to the HTTPs URL. Each key is a 512 bit storage key used for authentication when the storage account is accessed. The primary key is used for authentication while the secondary is used in place of the primary key until new sets of keys are generated.

- **Key Rotation**- Administrators can generate new sets of keys each time to avoid the keys being compromised by an attack but will have to deploy the new key to applications that use cloud storage services as backend where initially the old keys have been configured to use to access the cloud storage services. For instance, when an administrator renews the primary key, application using the key could use the secondary key pending the time a new key is generated to save downtime. Changing the storage account keys associated with a storage account is done via the Front End Layer using administrator's credentials.
- **Back up**- To backup data and files in Windows Azure, a backup vault or data store would be created in a geographic region where the data will be stored. This feature is available through the recovery services offered in Windows Azure that allows data to be backed up in the remote vault. Windows Azure offers the use of a certificate which is registered with the vault to allow data to be backed up or sent to the vault. The certificate also known as vault credentials, consists of a set of keys used to authenticate the machine that is being backed up to the remote vault. The public key is used to identify the machine which belongs to a vault while the private key is used to authenticate the backup process which are stored on the user's local machine. These credentials have a 48hr lifespan and are rotated to generate new sets of keys which are valid for recovery services.

The evaluation of Windows Azure is presented in Table 7.3 using the framework. Security parameters relevant to each layer of the cloud are mapped and security controls identified from the evaluation are shown in the Security Controls column.

TABLE 7.3: WINDOWS AZURE SECURITY EVALUATION

PaaS Layer	PaaS Component(s)	Security Threats	Security Requirement Domain	Security Methods	Security Mechanisms	Security Controls
Front End	Service Management Interface Web Portal	Service Level Threats	Identity and Access Management	Authentication/Authorization Methods Access Control Methods	Single Factor Authentication Multi-Factor Authentication Third Party Identity Authentication Role-Based/Mandatory Access Control	SSO OAuth 2.0 ADFS OTP SAS (Shares Access Token).
			Encryption + Key Management	Encryption Method Session Management	Asymmetric/Symmetric Encryption Key Distribution	PKCS12 X.509 certificates SSL AES-256
			Network Security	Auditing/Logging	Static/Proxy Firewall Packet Filters Network IDS/IPS	Application Firewalls. VPN IP Tunnelling

PaaS Layer	PaaS Component(s)	Security Threats	Security Requirement Domain	Security Methods	Security Mechanisms	Security Controls
Middle-Tier	App Container+ App DBMS Runtime Engine + SDK Abstraction +Operating System	Host Level Threats	Virtualisation Security	OS Patching Malware prevention/detection Auditing/Logging	Software Updates Anti-Malware	Windows Server Update Services (WSUS) Agentless Anti-Virus Microsoft Antimalware.
			Network Security	Data Monitoring Auditing/Logging Sandboxing/ Multi-tenancy	Data Isolation Mechanism Host IPS/ IDS Packet Filtering	Network ACLs. Windows Firewall. Barracuda (Proxy Web Application Firewall) Network Security Groups.
			Database Security	Encryption Method Data Recovery Methods	Asymmetric/Symmetric Encryption Backups/ Failover	AES 128, AES 192, AES 256, and Triple DES
			Encryption + Key Management			

PaaS Layer	PaaS Component(s)	Security Threats	Security Requirement Domain	Security Methods	Security Mechanisms	Security Controls
Back End	Platform Physical Resources + Repository DBMS	Infrastructure Level Threats	Database Security	Encryption Method Data Recovery Methods	Asymmetric/Symmetric Encryption Backups/ Failover	MD5 AES 128, AES 192, AES 256, and Triple DES
			Identity and Access Management	Authentication/Authorization Methods Access Control Methods	Single Factor Authentication Multi-Factor Authentication Third Party Identity Authentication Role-Based/Mandatory Access Control	SSO OTP Automated Phone Call. Network ACL
			Network Security	Data Monitoring Auditing/Logging Sandboxing/ Multi-tenancy	Data Isolation Mechanism Network IPS/ IDS Packet Filtering	Network ACLs Windows Firewall. Network Security Groups. ExpressRoute
			Encryption + Key Management	Encryption Method Key Distribution Data Recovery Methods Malware prevention/detection	Asymmetric/ Symmetric Encryption Custom Key Management Standard Key Management	MD5, AES 128, AES 192, AES 256, and Triple DES

Based on the security evaluation of security provisions offered on Windows Azure PaaS Cloud, results from the security provision analysis on each security domain are classified based on the security mechanism descriptions. Table 7.4 shows the classification of security mechanisms provided on each domain of Windows Azure using the classification criteria.

TABLE 7.4: SECURITY PROVISIONS –WINDOWS AZURE

Security Domain	Multi-Layered Security Mechanism Provision	Security Level	Classification
D1: Identity and Access Management	Multi-factor authentication: Single Factor + Second-Factor Non-biometric authentication mechanism. At least one or more access control policy implemented	Moderate	2
D2: Encryption and Key Management	Endpoint to endpoint Proprietary encryption with at least 192 –bit encryption keys (Data in Transit). Authentication and Key Exchange with at least 2048-bits encryption algorithm. Certificate issued by Third Party CA. Master Key Encryption Keys are managed by an internally hosted key management system/solution.	Moderate	2
D3: Virtualisation Security	Host Intrusion Detection System+ Automatic Operating System patches and driver updates + In-built proxy firewalls. System log enabled.	High	3
D4: Network Security	Network is accessible over specific IP address pool/Virtual Private Network Remote Access to Network restricted. Proxy Firewall-Packet Filtering Mechanism implemented. Network Intrusion Detection System implemented.	High	3
D5: Database Security	Database allocated into schemas (Data at Rest) All or Specific data tables and columns are stored in encrypted format/ Hash using proprietary encryption mechanisms. (Data at Rest) Data is encrypted using proprietary encryption. Data store keys are dynamically issued and stored within, protected by a Master Key (Data at Rest).	High	3

Security Provision Mapping

Windows Azure provides security features and mechanisms by default, while others have to be configured by the administrator. To evaluate whether the security provisions offered meets the customer security requirement specifications, we considered the following 4 steps:

1. Data from the classification of security provisions is mapped using the security mapping matrix.
2. A bar chart showing critical areas of focus where the security offerings have been implemented within the architecture is generated.
3. Mapping of security provisions is compared with security requirements mapping using bar charts.
4. Security provisions offered on each layer with regards to each security domain is compared based on the security mechanism description and classification.

Table 7.5 shows the classification of each requirement domain mapped into the matrix to identify critical areas in the cloud where security provisions are focused.

TABLE 7.5: CRITICAL SECURITY AREA OF FOCUS ANALYSIS (WINDOWS AZURE SECURITY PROVISIONS)

PaaS Layers	Security Management Responsibility			Security Domain					Critical Area of Focus
	Managed	Semi-Managed	Unmanaged	Identity and Access Mgt.	Encryption +Key Management	Virtualisation Security	Network Security	Database Security	
Front End	Provider	Provider	Customer	2	2	0	3	0	7
Middle-Tier	Customer/ Provider	Customer/ Provider	Customer	0	2	3	3	3	11
Back End	Provider	Customer	Customer	2	2	0	3	2	9
Prioritised Security Domain				4	6	3	9	5	

The data from the mapping matrix are used to generate a bar chart which clearly shows each security provision in each domain and the layer of the cloud architecture. The prioritised security domains where security are enhanced are also represented in the chart on the right (Figure 7.4).

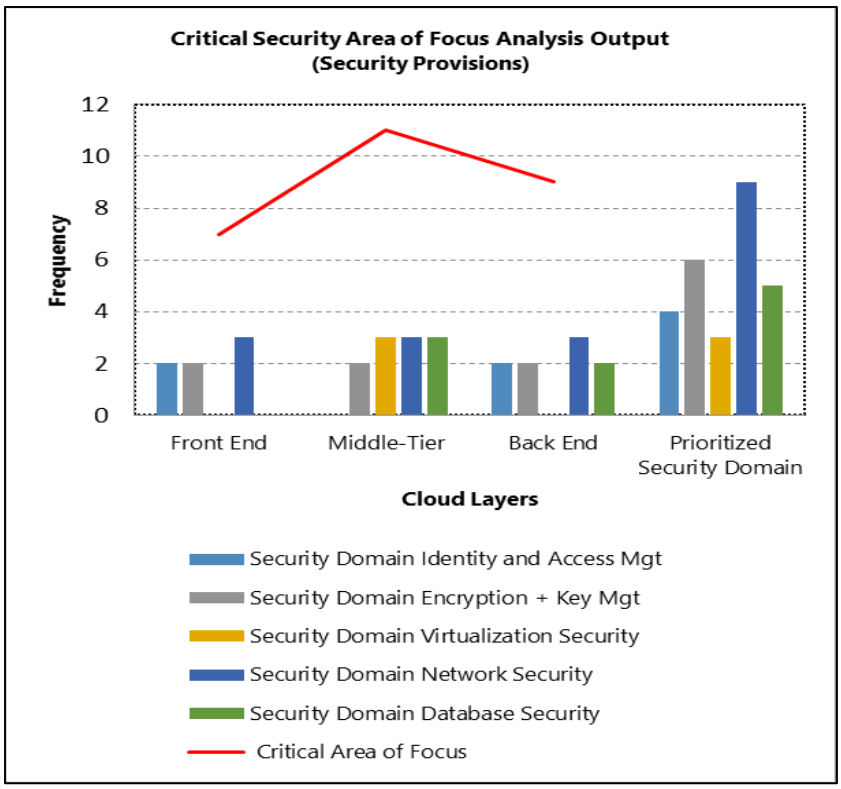

FIGURE 7.4: WINDOWS AZURE – SECURITY PROVISIONS CHART

SECURITY ASSESSMENT TEST (PAAS SECURITY MANAGEMENT CYCLE: PROCESS 7)

Identification of perceived vulnerabilities and threats in Windows Azure was limited to manual techniques alone. The use of security automated tools which include scanning and exploitation tools were not initiated. This is because permission and ethical l approval would have to be sought from

Microsoft in order to conduct tests on the cloud service. Hence reconnaissance and observations were considered the preferred evaluation methodology.

Security assessment was conducted in Windows Azure with emphasis on security domains to determine perceived threats to security requirements domains with the cloud architecture. A noticeable number of security vulnerabilities were found during the evaluation of the cloud service. The following security requirement domains were assessed and perceived vulnerabilities and threats were found.

TABLE 7.6 : PERCEIVED SECURITY VULNERABILITIES AND THREATS IDENTIFIED IN WINDOWS AZURE CLOUD LAYERS

Security Domain	**Cloud Layer**	**Security Assessment Technique**	**Security Mechanism(s):** SECURITY CONTROL(S)	**Perceived Vulnerabilities**	**Threat(s)**	**Vulnerability Validation**
D1: Identity and Access Management	Front End	Security Examination / Documentation Review	**Single-Factor Authentication:** SSO, WIF	**Inadequate Security Control Implementation:** - Compromise of login password credentials could allow malicious attacker have access to the SMAPI.	Service Level Threats- Authorized user account compromised. Intellectual property and data theft.	Yes
D3: Virtualisation Security	Middle-Tier	Security Examination	**Windows Updates :** WSUS	**Nature and Characteristics of PaaS Cloud Environments:** Windows Azure does not push Windows Updates to Windows Azure Virtual Machines since these machines are intended to be managed by the user.	Host Level Threats- Backdoor Attacks leading to compromised VMs. Trojan Attacks.	Yes

D4: Network Security	Middle-Tier	Security Examination	**Built-in Firewalls:** WINDOWS FIREWALL	**Core Technology Vulnerability:** Remote Desktop Protocol Vulnerability- Possibility of malicious attacker to remotely run codes due to the RDP being exploited.	Host Level Threats- Man in the Middle Attacks. Remote Code Execution.	No
D5: Database Security	Back End	Reconnaissance	**Single-Factor Authentication:** SSO, WIF **Key Distribution:** Internal HSM	**Nature and Characteristics of PaaS Cloud Environments:** Since the vault credentials is stored and managed by the cloud customer (user), there is the possibility of the vault credentials to be compromised or stolen by a malicious attacker	Infrastructure Level Threat- Registering machines against recovery service vault masked as an authorised user.	No

7.2.2 SCENARIO 2

Unmanaged Platform-as-a-Service Cloud

Alice is a lead IT administrator and security analyst for an application development SME. The SME has a security requirement paperwork and would want a cloud service that complies with industry standards such as ISO 27001/27002, SOC 1/SSAE 16/ISAE 3402 and SOC 2 and Cloud Security Alliance (CCM).The SME are considering adopting **Windows Azure Pack**, private (unmanaged) cloud environment where test applications can be developed before being pushed to a production environment for future releases. Alice and her team are required to evaluate the security offerings

on the private cloud to determine its capabilities and limitations and how it fits for purpose to meet security requirements highlighted by the SME.

Security Requirements Mapping (PaaS Security Management Cycle: Process 2)

D1. Identity and Access Management- The private cloud should enable the configuration of two-factor authentication for all users and the implementation of an external identity service for authentication. Access control policies should be integrated to allow authorised access on the management network for administrators only and deter unauthorised access. Features to enable the security of communication channels and endpoints using SSL or TLS should be available. Access to management and administration of cloud environment should be restricted only to the internal network and internal authorised users.

D2. Encryption and Key Management- Private Cloud should support the implementation of industry standard encryption such as AES 256-bit to encrypt data at rest and keys stored in a secure location protected by a key. Security feature should allow the rotation of encryption/decryption keys. The Private PaaS should enable the implementation of a certificate issued by a trusted certification authority with at least RSA-1024 bit encryption or higher.

D3. Virtualisation Security- Security feature should enable the isolation of tenant VMs. Proper secure boot technology must be integrated into the cloud platform to ensure proper hardware and software modules are authenticated before they are executed within the platform. Private PaaS must support the virtualisation memory firewall and antimalware to prevent untrusted application from allowing virus and worms from exploiting vulnerabilities.

D4. Network Security- Security feature must enable the monitoring of traffic to and from the cloud environment. Implementation of a secured Intrusion Detection System (IDS) that logs and alerts network traffic and issues relating to irregularities in the network and malicious attacks.

D5. Database Security- Security features that should enabled include the following

- The implementation of unauthorised access to database schemas and enforce row level data access.
- Minimise access to databases through the implementation of access control policies.
- Support the implementation of Transparent Data Encryption (TDE) using industry standard encryption algorithms.
- Enable the monitoring of the database store with firewalls to prevent database injections.

Security Requirements Analysis Output

With the use of the security level classification as shown in Table 7.7, the customer's security requirements are analysed and classified into the description categories of High, Moderate, Basic and None. The security requirement mapping framework is then used to identify critical security areas of focus in the PaaS cloud architecture. A bar chart of the security requirements analysis is then generated showing the critical area of focus using the mapping matrix.

TABLE 7.7: SCENARIO 2 -SECURITY REQUIREMENTS CLASSIFICATION

Security Domain	Security Mechanism Description	Security Level	Classification
D1. Identity and Access Management	Multi-factor authentication: Single Factor + Second-Factor Non-biometric authentication mechanism. At least one or more access control policy implemented	Moderate	2
D2. Encryption and Key Management	Endpoint to endpoint proprietary encryption with at least 256-bit encryption keys. (Data in Transit) Authentication and Key Exchange with at least 3072-bits encryption algorithm. Certificate issued by Third Party CA. All data are stored in encrypted format/Hash using proprietary encryption mechanisms. (Data at Rest). Master or Key Encryption Keys are managed on a dedicated external host with restricted access control policies.	High	3
D3. Virtualisation Security	Host Intrusion Detection System+ Automatic Operating System patches and driver updates + In-built proxy firewalls. System log enabled.	High	3
D4. Network Security	Network is accessible over specific IP address pool/Virtual Private Network Remote Access to Network restricted. Proxy Firewall-Packet Filtering Mechanism implemented. Network Intrusion Detection System implemented.	High	3
D5. Database Security	Database allocated into schemas (Data at Rest) Database is encrypted using proprietary encryption. All data tables and columns are stored in encrypted format/ Hash using proprietary encryption mechanisms. (Data at Rest). Data store keys are issued dynamically and stored externally protected by a Master Key (Data at Rest)	High	3

TABLE 7.8: CRITICAL SECURITY AREA OF FOCUS ANALYSIS (REQUIREMENTS SPECIFICATIONS)

PaaS Layers	Security Management Responsibility			Security Domain					Critical Area of Focus
	Managed	Semi-Managed	Unmanaged	Identity and Access Mgt.	Encryption +Key Management	Virtualisation Security	Network Security	Database Security	
Front End	Provider	Provider	Customer	2	3	0	3	0	8
Middle-Tier	Customer/ Provider	Customer/ Provider	Customer	0	3	3	3	3	12
Back End	Provider	Customer	Customer	2	3	0	3	3	11
Prioritised Security Requirement				4	9	3	9	6	

The data from the security mapping matrix can also be represented with a bar chart to highlight critical areas of focus in the PaaS cloud. Similar to scenario 1, security requirement specification for each security domain are clearly shown with the critical area of focus highlighted in the chart. The chart in Figure 7.5, indicates the Middle-Tier layer with frequency of 12 as the critical area where security requirements are more prevalent. Network and Encryption/ Key Management domains with security requirements with frequency of 9 respectively, appear to be the prioritised requirements in the scenario.

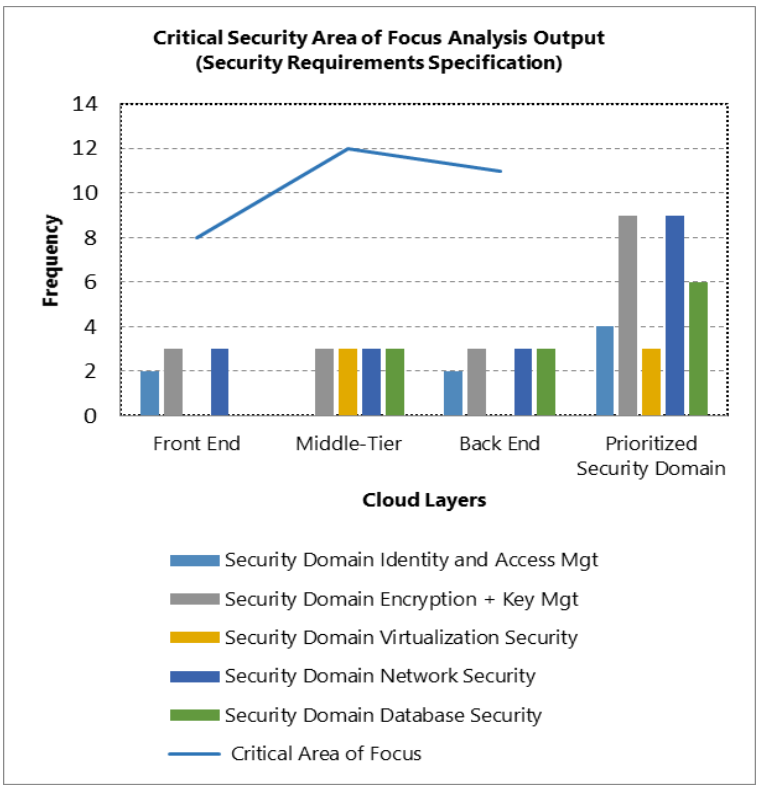

FIGURE 7.5: SCENARIO 2- CRITICAL AREA OF SECURITY OF FOCUS BAR CHART (REQUIREMENTS SPECIFICATIONS OUTPUT)

SEGREGATION OF WINDOWS AZURE PACK ARCHITECTURE (PAAS SECURITY MANAGEMENT CYCLE: PROCESS 3)

Windows Azure Pack is a PaaS private cloud offering provided by Microsoft. Based on Microsoft's Windows Azure technologies, the platform runs on a type 2 hypervisor host Windows Server 2012 R2 Operating System and Windows System Centre 2012. Similar to Windows Azure public PaaS model, Windows Azure pack provides capabilities for customers to setup a private cloud datacentre on premise and offer their tenants (customers) cloud services such as virtual machine clouds, website clouds, storage and networking services.

With the use of the reference model presented in Chapter 5, the PaaS cloud model is into three layers and components within each layer of the cloud are identified. The simulation and build of the private

cloud within a controlled laboratory environment, enabled adequate understanding of the architecture and segregation of this private PaaS cloud into layers. It also enabled the identification of existing components and technologies that provide the service. The simulation was configured using hardware that consists of servers joined in a domain and are dedicated to provide services and functionalities within the private cloud architecture.

Layer 1- Front End: This layer comprises of a user interface which allows administrators and their tenants to manage and configure cloud services depending on their roles within the cloud architecture. This layer offers functionalities through a Service Management Application Programming Interface (SMAPI) or through the use of Windows Power Shell command prompt. These interfaces are RESTful APIs that are set using the port numbers to issue URL requests. There are two SMAPIs used by administrators and tenants to manage resources on the private cloud platform.

Service Management Application Programming Interface (SMAPI)/ Web Portal

Windows Azure Pack Admin Management Portal – Enables the administrator to complete management tasks through the management portal user interface. The API serves as a management portal for administrators to manage cloud resources, create user accounts and subscriptions as well as interact with the cloud internal components and security configurations.

Windows Azure Pack Tenant Management Portal – Enables tenants to manage their subscription web and cloud services provisioned on Windows Azure pack. It also serves as the interface for which service management can be performed which includes the creation of web applications, virtual machines and storage databases.

Both interfaces were provisioned by a dedicated server**, wap.cloud.local,** which hosts the Windows Azure Pack Express Installation and running on Windows Server 2012 R2 operating system. The server hosts the server management APIs which include the Windows Azure Pack Tenant API, a dedicated Tenant public API which is exposed to the internet to allow tenants access to the management portal. The server also hosts the administrator's management portal which includes the Windows Azure pack Admin API and an internal Tenant API which is not exposed to the internet.

Layer 2- Middle Tier: This layer consists of components that serve as the runtime environment, SDK for web application developments which is then deployed and hosted on application containers relative to storage containers and databases. It also consists of the abstraction and operating systems that enable services to be hosted and provisioned with the cloud architecture. The components that provision these capabilities on the private PaaS are described below:

a) **Runtime Environment**- This component is provisioned by dedicated servers that host virtual machine and web application cloud services. These servers include the SPF server, VMM server, and Runtime Database Server.

   Service Provider Foundation (SPF) – enables tenants to access virtual machine services through the Front End by interacting with the VMM that hosts the virtual machine resources. The VM services also known as the IaaS service is provisioned by the Service Provider Foundation.

   Virtual Machine Manager (VMM) – manages the PaaS Virtual Machines, host virtual machines and operating system images which provides services for the creating of tenant virtual machines.

Runtime Database- Comprises of a database that supports tenant developed and deployed applications within the cloud service. This includes website clouds and virtual machine clouds.

b) **Application Container and DBMS**- The Web Application Services consists of PaaS Services that are provided by the servers in the **Server Farm**. These servers have individual roles that host resources and files for developed and deployed web applications. Hence they serve as application containers, database servers for tenants as well as end point communication channels to deployed applications which can be accessed by the end users. Although these servers can be hosted by physical servers, in our simulation, the web application services were hosted by virtual machines joined to the domain "cloud.local".

c) **Abstraction and Operating System**- This component is serviced by the hypervisor that provisions VMs using the VMM hosted by a server. The abstraction on our simulation build was hosted by Windows Hyper-V which serves as the abstraction between the Runtime environment and the underlying physical resources provisioned on the Back End layer.

Layer 3- Back End: Windows Azure Pack is supported by underlying physical resources that support the entire PaaS cloud architecture. From the private cloud simulation, the Back End component consists of servers in a domain which includes the following:

a) **Physical Platform Resources-** This component is serviced by a collection of servers as part of the infrastructure level of the cloud architecture. The servers and their functions are described as follows:

- **Domain Controller (DC) Server** – DC manages identity of other servers in the domain through Active Directory and Active Directory Federated Services (ADFS) installed.
- **VMM Server**- Hosts the System Centre Virtual Machine Manager.

- **Hyper-V Host Server**- Hosts the Abstraction Type-2 Native Hypervisor.

b) **PaaS Database Management System (DBMS)**:

- ***SQL Service Management Database Server-*** serves as a failover cluster as well as instances for Windows Azure Services and serves as database for the VMM Server.

Figure 7.6 below shows the segregated layers of Windows Azure Pack and its components using the PaaS cloud Reference Model presented in Chapter 5.

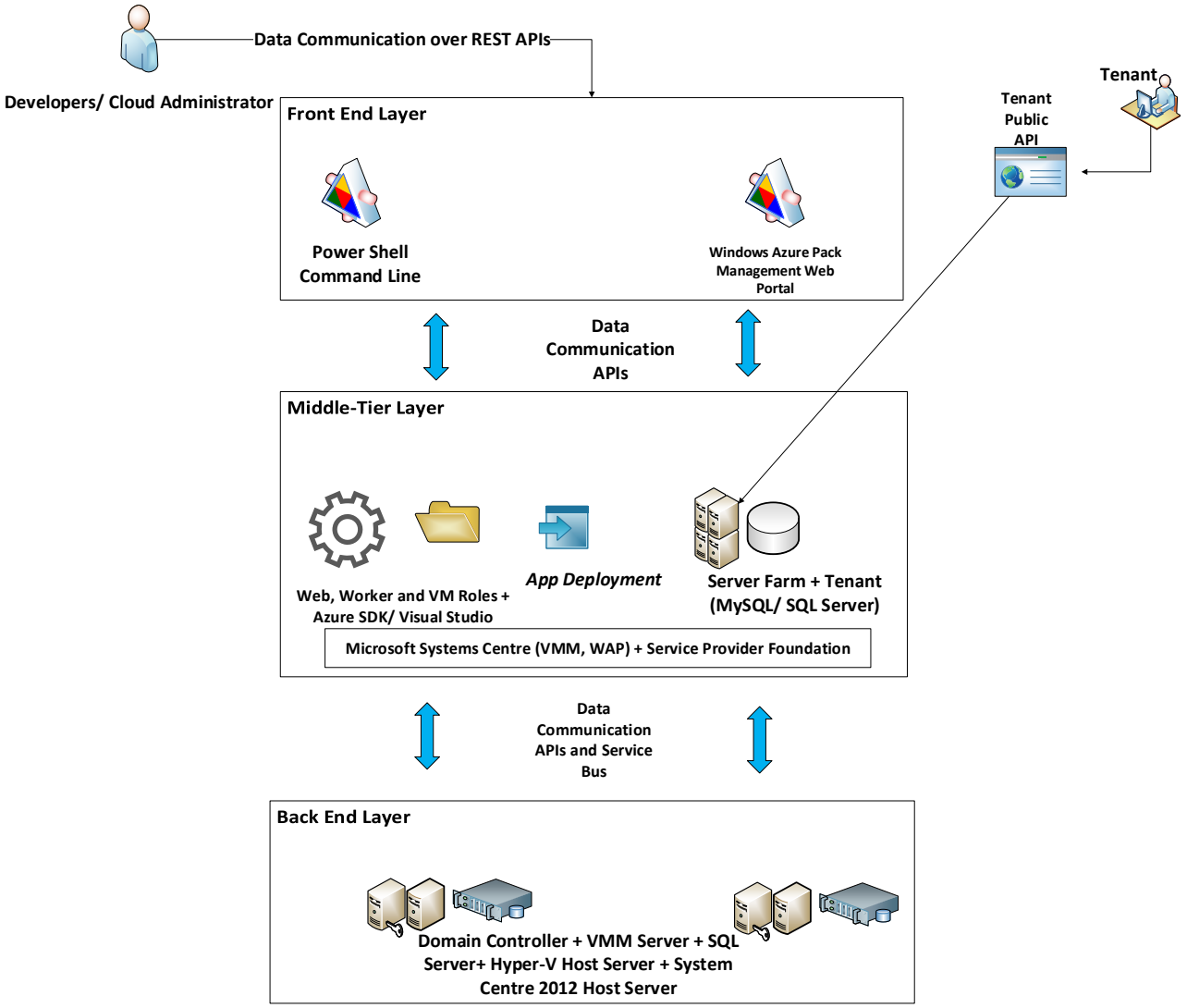

FIGURE 7.6: WINDOWS AZURE PACK- PAAS CLOUD ARCHITECTURE AND COMPONENTS (REFERENCE MODEL ILLUSTRATION)

SECURITY EVALUATION OF WINDOWS AZURE PACK

(PAAS SECURITY MANAGEMENT CYCLE: PROCESS 4, 5, 6)

Security scan of Windows Azure Pack was conducted using the Microsoft Baseline Configuration Analyser 2.0 software tool to gather information about the security implementations across the cloud architecture. Figure 7.7 shows a screenshot taken from the use of the analyser to evaluate Windows Azure Pack installation and configuration on our private cloud proof of concept.

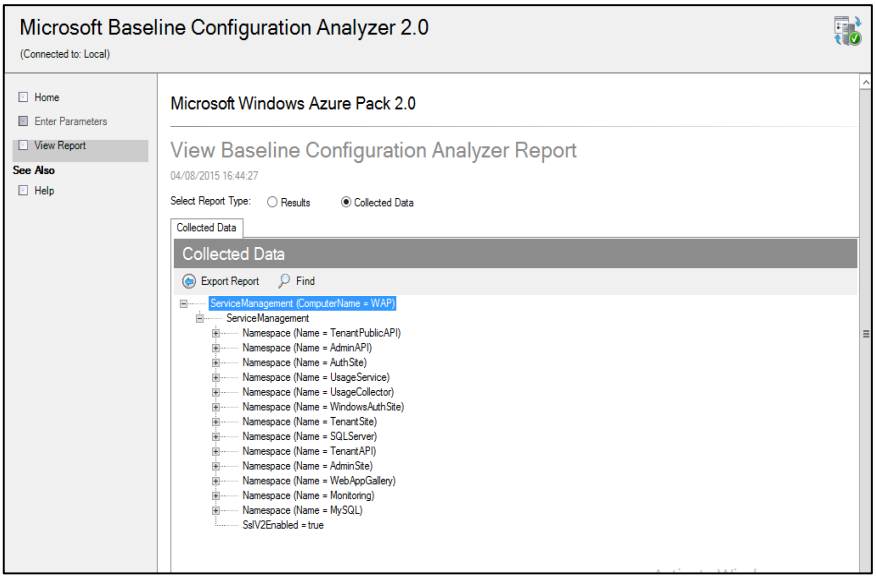

FIGURE 7.7: SECURITY CONFIGURATIONS IMPLEMENTED IN WINDOWS AZURE PACK

A clear description of security implementations found across each security domain are described in detail:

D1. Identity and Access Management

Identity and Access Management of Windows Azure Pack is facilitated with the configuration of **Identity Providers** using different security features and mechanisms. They include:

a. **Active Directory Federation Services (ADFS) –** Windows uses ADFS through the Domain Controller (DC) to server as an identity provider for computers and users joined to the domain. This security is available and needs to be configured to ensure both the management portal and tenant management sites on the Front End trust ADFS for authentication and authorisation of credentials. Once the security feature is added on the DC, the portals can therefore be configured to trust ADFS. This is enabled by running the respective lightweight command "***Set-MgmtSvcRelyingPartySettings***" from Windows PowerShell on servers hosting the management and tenant portals.

b. **Secure Token Service (STS) –** Secure communication between components at the Front End and Middle Tier layers on Windows Azure Pack is provisioned by claim based token and a basic authentication to validate user credentials from the Front End to ensure secure communication to components in the Middle Tier handled by the Service Foundation Provider. Once a user (management or tenant) logs in at the front end, the portal redirects the user to a STS which in turn redirects the user to a login page where credentials are entered.

   Once the credentials are validated, a claim based token is issued which is added to the user's URL and timed. It is then passed on to the SMAPI which authenticates the user with access to the Middle Tier layer with assistance from the SPF using basic authentication.

   The SPF governs access control using a Role Based Access Controls (RBAC) based on user credentials stored in the Service Management Database at the Back End layer.

D2. Encryption and Key Management

Security features for encryption on Windows Azure Pack are provisioned using encryption keys, algorithms and passwords to secure endpoint communication and data security. The following are the security features provisioned on Windows Azure:

- **Asymmetric Encryption (Data in Transit)** – Windows Azure Pack provides security of the communication channels and endpoint through SSL and TLS asymmetric cryptographic protocols to ensure data integrity. This requirement complements network security using X.509 certificates by ensuring packets received during the communication have not been modified as servers in the domain during communication compare hashes of encrypted data received to see if there is a match. If not the packets are dropped or destroyed. The configuration of SSL and TLS are not enabled by default and have to be configured and implemented on the cloud service. The encryption algorithm and keys used during encryption have to be rotated manually by the administrator and key securely in a configuration store secured using a machine key.

  Encryption Algorithm Use is AES with a key size of 256. Authentication and Validation of credentials uses SHA 256 with a Key Size of 512. These resources were gathered based on the use of self-signed certificates.

  Security of the Service Provider Foundation ensures only encrypted calls are made through dedicated HTTPS ports and that only such encrypted requests are accepted. The security mechanism used SSL asymmetric encryption on the data communication channels and that only authorised credentials registered on the domain have privileges to make such requests.

- **Symmetric Encryption (Data at Rest)** – Database resources in Windows Azure Pack are hashed and stored in rows and columns within schemas of the database server. Access to the database is protected using a password which is authenticated using Windows authentication which is preferred to a mixed mode authentication. Kerberos can also be enabled to provide enhanced security that is based on master keys and encrypted tickets.
- **Distributed Key Management**- During installation of the VMM Server, Windows Azure Pack through Microsoft System Centre provides the option of storing encryption keys used to encrypt data on the VMM server or on the Domain Controller. To enable distributed key management, encrypted credentials, VMM roles as well as VMM disk property resources are encrypted by default by performing a symmetric encryption on the RSA asymmetric encryption keys used to encrypt data. This process requires a simple cryptographic application programming interface called Data Protection Application Programming Interface (DPAPI), available to Windows Servers including Windows Server 2012 R2 used in the build simulation. The cryptographic keys are stored in a container on the DC which has to be manually created by the administrator during installation.

D3. Virtualisation Security

- **Disaster Recovery**- Windows Azure provides failover recovery for the Hypervisor, Hyper-V Host and VMM Server, by provision of the Hyper-V Recovery Manager which prevents data loss during OS patching of the VMM. The Recovery Manager has to be manually downloaded and installed on the VMM Server that hosts and provisions VMs or can be automated to monitor any changes in the environment prompt the replication through the Recovery

Manager. It creates a replica of the VMs in a VM cloud in case of a failover or recovery in case of an outage by replicating the environment to a secondary location.

- **OS Patching**- Through automatic and manual security updates on Windows Servers, Windows Azure Pack operating systems are updated with regular security updates to ensure the latest versions are installed are up to date. These include Service packs, hotfixes and security patches. It requires that servers in the Windows Azure Pack private cloud architecture having an endpoint connection with the public internet to enable these updates to be downloaded and installed.
- **Third Party Virtualisation Security**- Hyper-V security on Windows Azure Pack can be configured with security solutions such as "5nine Cloud Security" for Hyper-V. It is an agentless security solution that provides Intrusion Detection System (IDS) as well as antivirus and firewall security on Hyper-V environments. In as much as "5nine Cloud Security" provides security on the Hypervisor, it also supports tenant security integration to provide security as a services for tenant VMs.
- **Security Monitoring and Audit**- Security monitoring and assessment on Windows Azure Pack can be initiated with the use of the Microsoft Baseline Security Analyser. The software tool helps to assess security updates and settings of components within the cloud environment. The software has to be downloaded and then used to scan servers that have Windows Azure Pack components installed on them. These include the System Centre Host Servers that host the WAP, SPF and VMM. A security report is then generated with a list of resolution that described the audit and analysis result.

D4. Network Security

Network Security is enhanced on Windows Azure pack through several security features and security configuration. They include:

- **IP Filtering** – To prevent infrastructure and service level threats such as DoS attacks. The configuration in our simulation required setting a range of IP addresses that can access the web site cloud. This also helps prevent unauthorised access through the network to servers in the cloud.
- **Setting Quotas**- Quotas were set through the Front End management portal to prevent DoS attacks to stop excess traffic sent to web applications hosted in application containers. The process involves halting traffic during a DoS attack by stopping network traffic been fed to the server hosting the resource.
- **Firewall Configuration**- By default, Windows servers have host-based firewalls that can be configured to monitor network traffic to and from servers hosting services in Windows Azure Pack architecture. The host firewall only responds to inbound traffic and restricts unsolicited network traffic once firewall rules are set.
- **IP Security**- Windows Server Firewall security is equipped with IP security feature to configure various connection security services to network traffic. It involves setting rules in Windows Firewall with Advanced Security that detects the characteristics of the network traffic to protect, and the nature of the protection to be applied. It also enables the configuration of encrypting data packets that travel through communication channels and endpoints with the use of cryptography. This ensures that integrity of data packets sent through the channels

are maintained and prevents service level and infrastructure level threats for instance Man-in-the-Middle attacks.

- **Virtual Networks**- Windows Azure Pack allows the configuration of virtual networks to isolate VMs and resources within the multi-tenant cloud environment. In this way, data isolation is initiated and also reduces the chances of IP address conflicts as VMs on different subnets can have the same IP address without any network conflict and configuration. The virtual local area network configuration on Windows Azure Pack supports the IEEE 802.1Q standard that supports the tagging of Ethernet frames.

D5. Database Security

Database security on Windows Azure Pack are provisioned via the following security features:

- **Single Factor Authentication** – All server on Windows Azure Pack which include the application container DBMS, tenant database and the service management database on both the Middle-Tier and Endpoint layers are safeguarded using a single factor authentication method using passwords. The passwords have to be configured during installation of the database servers and have to be changed or rotated to ensure security. All physical resource providers at the Back End DBMS and Middle Tier DBMS are protected using passwords which have to be rotated or changed to provide data integrity and confidentiality. It requires running some commands in Windows PowerShell command line on each of the database servers.
- **Backup**- PaaS cloud services and resources can be backed up on Windows Azure Pack. This also includes VMM database, VMs, encryption keys and credentials. For website cloud services, the backup involves backing up the Server Farm Website Controller, Runtime

Database and the File Server in the Middle Tier Layer. It involves running command line scripts on Windows PowerShell.

Moreover, the VMM and its resources can be backed up and restored. This involves backing up the SQL Service Management Database which hosts the VMM database and resources necessary for administrator and tenant accounts to run. However, backup has to be done manually as the administrator with privilege account has to run scripts on the service management database. The File Server which hosts website contents and web applications resources developed and deployed by the cloud tenants can be backed up by running a script using administrative privileges to backup individual tenant files and folders stored on the server.

In Table 7.9, the output from the evaluation of security mechanism and controls implemented in Windows Azure Pack are presented in a table. The table clearly shows the security controls implemented by default and also those that cloud be configured in each cloud layer.

TABLE 7.9: WINDOWS AZURE PACK: SECURITY EVALUATION FRAMEWORK OUTPUT

PaaS Layer	PaaS Component(s)	Security Threats	Security Requirement Domain	Security Methods	Security Mechanisms	Security Controls
Front End	Service Management Interface Web Portal	Service Level Threats	Identity and Access Management	Authentication/Authorization Methods Access Control Methods	Single Factor Authentication Identity Provider Authentication Role-Based Access Control	ADFS 2.0 Passwords STS Tokens
			Encryption + Key Management	Encryption Method Session Management	Asymmetric/Symmetric Encryption Key Distribution	SSL/TLS Internal HSM
			Network Security	Auditing/Logging	Static/Proxy Firewall Packet Filters Network IDS/IPS	Windows Advanced Firewall Microsoft Security Analyser

PaaS Layer	PaaS Component(s)	Security Threats	Security Requirement Domain	Security Methods	Security Mechanisms	Security Controls
Middle-Tier	App Container+ App DBMS Runtime Engine + SDK Abstraction +Operating System	Host Level Threats	Virtualisation Security	OS Patching Malware prevention/detection Auditing/Logging	Software Updates Anti-Malware Third Party Virtual Appliances	Windows Automatic Updates Windows Security Essential 5nine Virtual Appliance and Agentless Anti-virus
			Network Security	Data Monitoring Auditing/Logging Sandboxing/ Multi-tenancy	Data Isolation Mechanism Host IPS/ IDS Packet Filtering	VLANs IP Sec/ IP Tunnel
			Database Security	Encryption Method Data Recovery Methods	Asymmetric Encryption Backups/ Failover	SSL/TLS Hyper-V Recovery Manager
			Encryption + Key Management	Encryption Method Session Management Key Distribution	Asymmetric Encryption Key Distribution	SSL/TLS Internal HSM

PaaS Layer	PaaS Component(s)	Security Threats	Security Requirement Domain	Security Methods	Security Mechanisms	Security Controls
Back End	Platform Physical Resources + Repository DBMS	Infrastructure Level Threats	Database Security	Encryption Method Data Recovery Methods	Symmetric Encryption Backups/ Failover	SHA 256 Windows Authentication
			Identity and Access Management	Authentication/Authorization Methods Access Control Methods	Single Factor Authentication Role-Based Access Control	Passwords Kerberos Domain GPO
			Network Security	Data Monitoring Auditing/Logging Sandboxing/ Multi-tenancy	Data Isolation Mechanism Network IPS/ IDS Packet Filtering	VLANs IP Sec IP Tunnelling
			Encryption + Key Management	Encryption Method Key Distribution Data Recovery Methods Malware prevention/detection	Symmetric Encryption Standard-Key Management	SHA 256 Internal HSM Windows Server Backup Agentless Antivirus

Security Provision Mapping

Windows Azure Pack provides security features and mechanisms by default, while others have to be configured by the administrator. To evaluate whether the security provisions offered meets the customer security requirement specifications, we considered the following 4 steps which are identical to the mapping procedure used in scenario 1:

1. Data from the classification of security provisions is mapped using the security mapping matrix.
2. A bar chart showing critical areas of focus where the security offerings have been implemented within the architecture is generated.
3. Mapping of security provisions is compared with security requirements mapping using bar charts.
4. Security provisions offered on each layer with regards to each security domain is compared based on the security mechanism description and classification.

Table 7.10 shows the security provisions and mechanisms implemented in Windows Azure Pack. The security level for and classification for each security domain are also clearly shown.

TABLE 7.10: SECURITY PROVISIONS –WINDOWS AZURE PACK

Security Domain	Multi-Layered Security Mechanism Provision	Security Level	Classification
D1: Identity and Access Management	Single Factor Authentication + Single or multiple access control policy.	Basic	1
D2: Encryption and Key Management	Endpoint to endpoint Proprietary encryption with at least 192 –bit encryption keys (Data in Transit). Authentication and Key Exchange with at least 2048-bits encryption algorithm. Certificate issued by Third Party CA. Master Key Encryption Keys are managed by an internally hosted key management system/solution.	Moderate	2
D3: Virtualisation Security	Host Intrusion Detection System+ Automatic Operating System patches and driver updates + In-built proxy firewalls. System log enabled.	High	3
D4: Network Security	Network is accessible over specific IP address pool/Virtual Private Network Remote Access to Network restricted. Proxy Firewall-Packet Filtering Mechanism implemented. Network Intrusion Detection System implemented.	High	3
D5: Database Security	Database allocated into schemas (Data at Rest) All or Specific data tables and columns are stored in encrypted format/ Hash using proprietary encryption mechanisms. (Data at Rest) Data is encrypted using proprietary encryption. Data store keys are dynamically issued and stored within, protected by a Master Key (Data at Rest)	Moderate	2

Table 7.11 shows the classification of each requirement domain mapped into the matrix to identify critical areas in the cloud where security provisions are focused.

TABLE 7.11: CRITICAL SECURITY AREA OF FOCUS ANALYSIS (WINDOWS AZURE PACK SECURITY PROVISIONS)

PaaS Layers	Security Management Responsibility			Security Domain					Critical Area of Focus
	Managed	Semi-Managed	Unmanaged	Identity and Access Mgt.	Encryption +Key Management	Virtualisation Security	Network Security	Database Security	
Front End	Provider	Provider	Customer	1	2	0	3	0	6
Middle-Tier	Customer/ Provider	Customer/ Provider	Customer	0	2	3	3	2	10
Back End	Provider	Customer	Customer	1	2	0	3	2	8
Prioritised Security Provision				2	6	3	9	4	

The data from the mapping matrix are used to generate a bar chart which clearly shows each security provision in each domain and the layer of the cloud architecture. The prioritised security domains where security are enhanced are also represented in the chart (Figure 7.8).

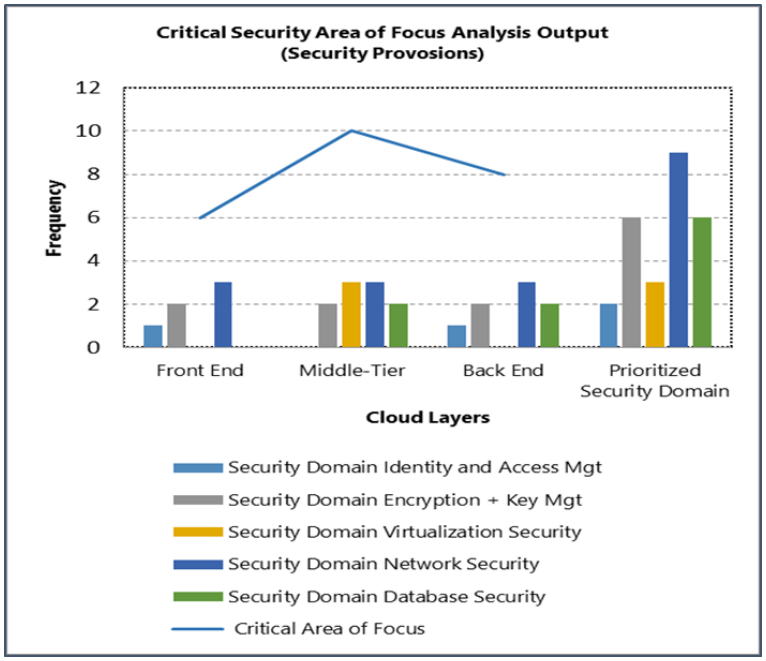

FIGURE 7.8: WINDOWS AZURE PACK-SECURITY PROVISIONS CHART

SECURITY ASSESSMENT TEST (PAAS SECURITY MANAGEMENT CYCLE: PROCESS 7)

Security evaluation and assessment was conducted in Windows Azure Pack post installation and configuration of security implementations using the chosen automated tools. The Microsoft Baseline Security Analyser and Microsoft Baseline Configuration Analyser tools were used to scan the security of the entire cloud service, host and infrastructure environment for vulnerabilities and threats.

The Nessus vulnerability scanner was also deployed to explore vulnerabilities of security implementation and impact within the cloud architecture.

The results showed the configuration and security implementations were configured properly in accordance with security principles adequate for a proof of concept controlled environment for test and analysis purposes. However, security threats were found due to vulnerabilities found in the cloud architecture. Manual technique were then deployed to exploit of these vulnerabilities in order to validate the security vulnerabilities found in each layer of the PaaS cloud. A detailed report of the assessment and validation test is provided in the subsequent sub-sections.

a. Configuration Analysis of Windows Azure Pack Environment

A configuration scan was carried out on Windows Azure Pack using the Microsoft Baseline Configuration Analyser. Out of a total of 357 results gathered, 41 items were tagged as non-compliant with adequate configuration settings. (See Figure 7.9). The severity level on each scanning result issued can be classified into three (Table 7.12).

TABLE 7.12: MBCA SEVERITY LEVEL

Severity Level	Description
Non-Compliant	The component does not satisfy the conditions of a rule
Compliant	The component satisfies the conditions of a rule
Warning	The component is compliant as it is operating currently but might not satisfy the conditions if changes are made to its configuration or policy settings.

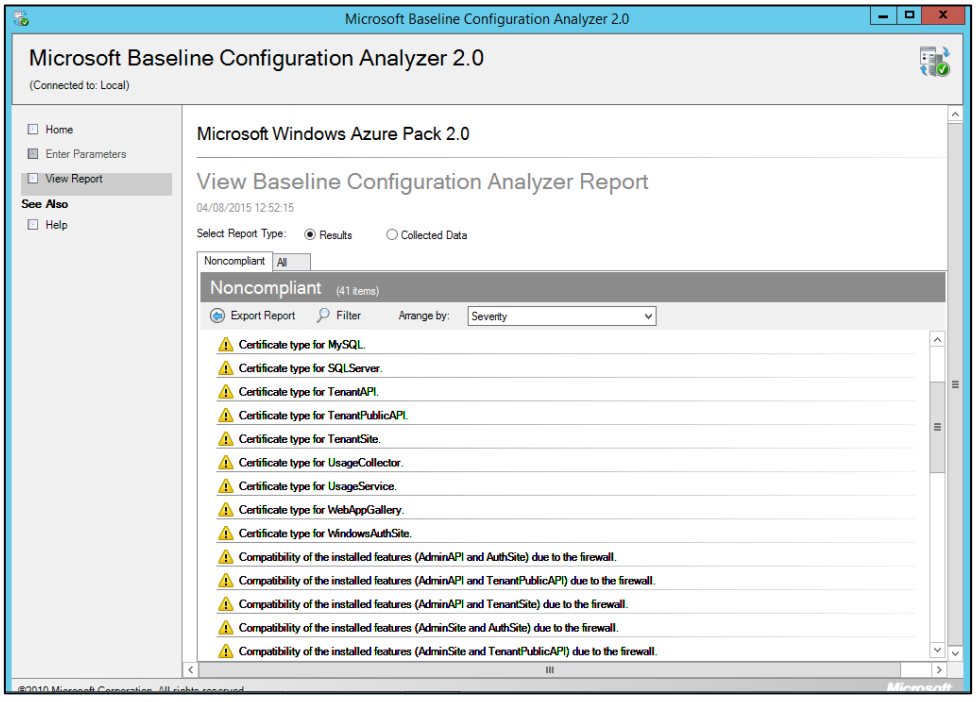

FIGURE 7.9: MBCA CONFIGURATION SCAN SHOWING NON-COMPLIANT WARNINGS WITHIN WAP

The scan results offered resolutions to resolve the security issues identified during the scan. The resolutions could either be excluded, fixed due security implementations which were either not properly configured, missing or inadequate.

b. Security Analysis of Windows Azure Pack Infrastructure

With the use of Microsoft Baseline Security Analyser (MBSA), a scan on the architectures of the cloud environment was conducted after security implementations were configured. The initial results from the scan identified a number of security issues which include security updates that needed to be installed on individual servers in the private PaaS cloud simulation. These included administrative password issues and security updates that needed to be installed.

Once the updates were installed, a scan was again conducted which satisfied all security updates were installed and security settings within the cloud architecture had been met.

A detailed report of the security scan reports can be found in the appendices (See Appendix C).

c. Nessus Vulnerability Scan- Cloud Infrastructure Audit

Vulnerability audit scan was conducted using Nessus 6.4 to scan for vulnerabilities in the PaaS cloud architecture. The severity of vulnerabilities were categorised into Critical, Medium and Low. The results were similar to scan results obtained using the MBCA. A detailed report of the scan and vulnerabilities found can be seen in the Appendix C.

A detailed security assessment was conducted on Windows Azure Pack to assess security vulnerabilities that could allow possible threats and attacks that could compromise information security of data and resources in the cloud. The assessment was conducted by exploiting security vulnerabilities which were exposed due to the inadequate security provisions that are offered in each layer of the cloud. Table 7.13 below, highlights the vulnerabilities on Windows Azure Pack and

threats that risk the preservation of the confidentiality, availability and integrity of data and resources in the private cloud environment.

Vulnerabilities

Similarly, a number of non-compliant warnings emerged which showed security vulnerabilities within the configuration of the WAP.

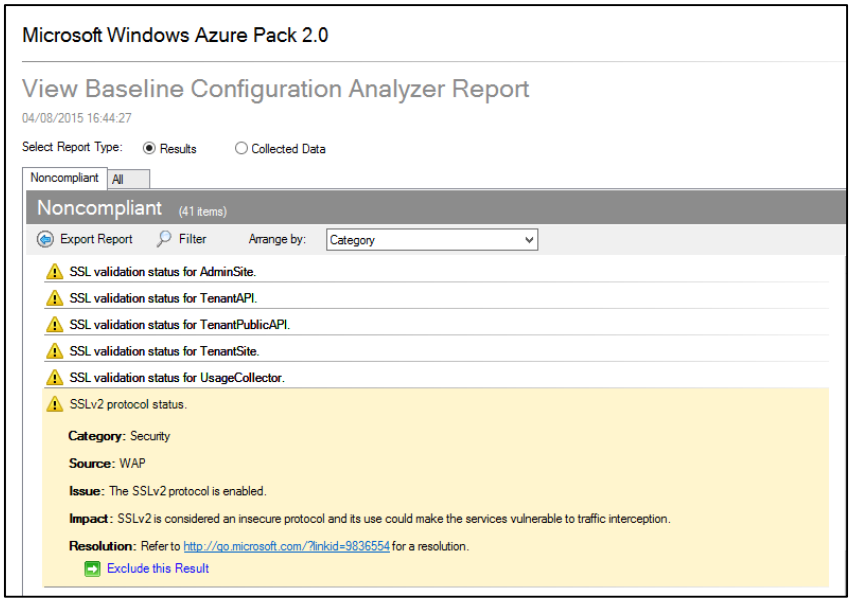

FIGURE 7.10: SSLV2 PROTOCOL WARNING

Issue- Inadequate Security Control Implementation/ Security Control Defect:

The above warning indicates that SSL version 2 is enabled by default in the configuration.

Impact (Severe): SSL version 2 is considered an insecure protocol and could make services vulnerable to man-in the-middle attacks and poodle attacks.

Resolution: Disabling the protocol on the WAP Server.

Action Taken: Disabled the SSLv2 on the registry of WAP server.

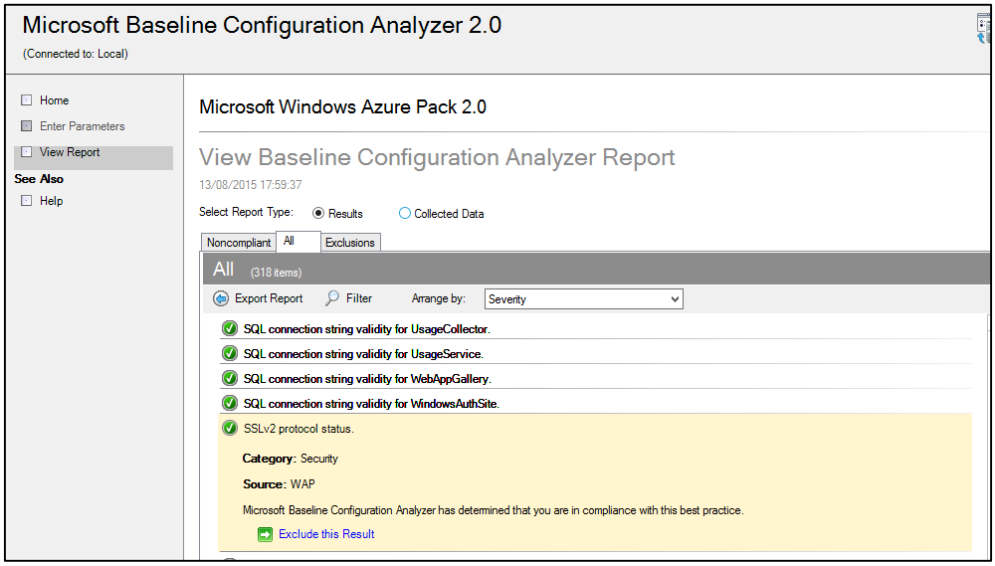

FIGURE 7.11: SSLV2 PROTOCOL DISABLED AND IN COMPLIANCE WITH CONFIGURATION SETTINGS

Issue: Tenant SQL password can be changed by attacker with authorised log in credentials through the tenant portal without prompting for old password.

Impact (High): Service unavailable to tenant and possible data leakage.

Exploit: Change user password to deny access to the DBMS after gaining authorised access.

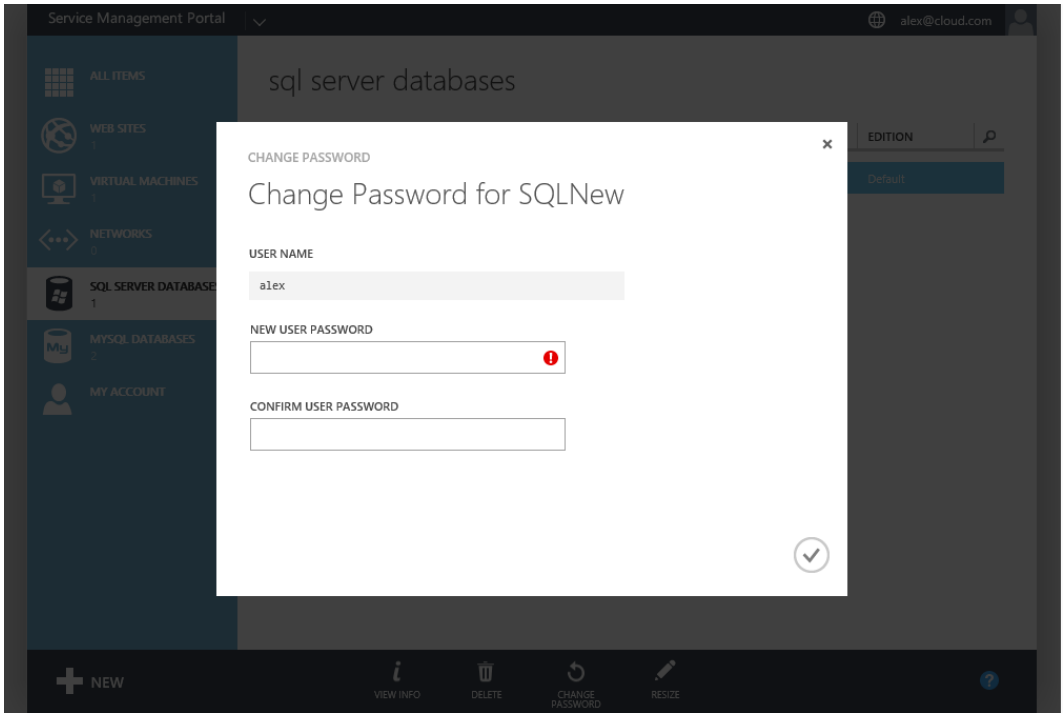

FIGURE 7.12: SQL PASSWORD CHANGE PROMPT ON WINDOWS AZURE PACK

Issue: Publish Settings for cloud web app download contains unencrypted credentials.

Impact (High): Service unavailable to tenant and possible data leakage.

Exploit: credential theft for unauthorised access to tenant database using unencrypted connection string.

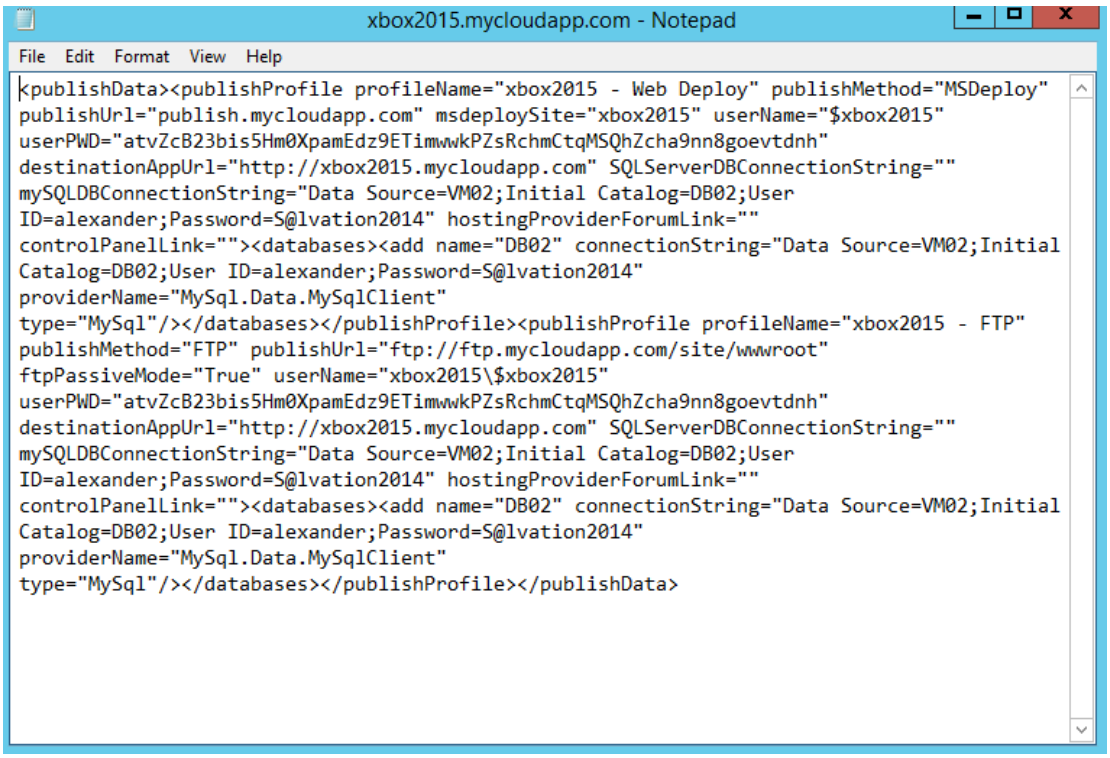

FIGURE 7.13: PUBLISH SETTINGS DOWNLOADED FROM TENANT SMAPI

The table shows a detailed list and description of vulnerabilities found on each layer of Windows Azure Pack PaaS cloud environment and threats associated with each vulnerability. The security mechanisms and controls implemented in each layer which failed to prevent the threats after vulnerability validation tests were conducted through security exploitation.

TABLE 7.13: SECURITY VULNERABILITIES AND THREATS IDENTIFIED IN WINDOWS AZURE PACK CLOUD LAYERS

Security Domain	Cloud Layer	Security Assessment Technique	Security Mechanism(s)	Vulnerabilities	Threat(s)	Vulnerability Validation
D1: Identity and Access Management	Front End	Reconnaissance	**Single-Factor Authentication:** ADFS 2.0 Passwords STS Tokens	**Inadequate Security Control Implementation:** Compromise of login password credentials could allow malicious attacker have access to the SMAPI.	Service Level Threats- Authorized user account compromised. Intellectual property and data theft. Distributed Denial of Service (DDOS).	Yes
	Middle-Tier	Privilege Elevation Security Examination	**Single-Factor Authentication:** ADFS 2.0 Passwords STS Tokens	**Core Technology Vulnerability:** By default, application source code settings also known as publish settings can be downloaded through the tenant portal as it contains username, password and database connection string credentials.	Service Level Threats- Distributed Denial of Service (DDOS). Information Leakage and Data theft.	Yes

	Back End	Privilege Elevation Security Examination	**Single-Factor Authentication:** ADFS 2.0 Passwords STS Tokens	**Inadequate Security Control Implementation:** Single-Factor Authentication- Compromise of login password credentials could allow malicious attacker have access to the platform physical DBMS without a strong authentication mechanism implemented to validate user identity.	Service Level Threats- Authorized user account compromised. Intellectual property and data theft. Distributed Denial of Service (DDOS).	Yes
D2: Encryption and Key Management	Front End	Security Scan	**Asymmetric Encryption**: SSL v2 and SSL v3	**Inadequate Security Control Implementation/ Security Control Defect:** By default, SSL v2 and SSLv3 are enabled in Windows Azure Pack.	Service Level Threats- Man in the Middle Attacks. Length Extension Attacks. Poodle Attacks.	Yes
	Back End	Security Scan	**Key Distribution:** Internal HSM	**Core Technology Vulnerability:** Key management system on Windows Azure Pack allows for encryption keys to be stored within in the configuration file which serves as an internal HSM for the cloud platform. Hence making the keys vulnerable to possible unauthorised access.	Host Level Threats- Data Leaks. Stolen Database backups.	No
D3: Virtualisation Security	Middle-Tier	Privilege Elevation Security Scan	**Single-Factor Authentication:** ADFS 2.0	**Core Technology Vulnerability:** Remote Desktop Protocol Vulnerability- Possibility of malicious attacker to remotely run codes due to the RDP being exploited.	Host Level Threats- Man in the Middle Attacks. Remote Code Execution.	No

		Security Scan	**Single-Factor Authentication:** ADFS 2.0	**Inadequate Security Control Implementation:** Home web application cloud credentials can be edited by attacker with authorised access through the SMAPI. Which allows Middle-Tier Layer services to be compromised.	Service Level Threat- Distributed Denial of Service (DDOS)	Yes
D5: Database Security	Back End	Privilege Elevation	**Key Distribution:** Internal HSM **Single Factor Authentication:** Windows Authentication	**Nature and Characteristics of PaaS Cloud Environments:** Since the vault credentials is stored and managed by the cloud customer (user), there is the possibility of the vault credentials to be compromised or stolen by a malicious attacker.	Infrastructure Level Threat- Registering machines against recovery service vault masked as an authorised user.	Yes
	Middle-Tier	Security Examination/ Privilege Elevation	**Single-Factor Authentication:** Windows Authentication	**Core Technology Vulnerability:** Changing of tenant database string credentials which can be used to access to database remotely.	Host Level Threats- Distributed Denial of Service (DDOS). Intellectual property and data theft. Remote Code (Query) execution initiated within the application DBMS.	Yes

7.3 SUMMARY

Segregation of Windows Azure and Windows Azure Pack using the reference model from the scenarios enabled the identification of components in each cloud architecture. It also enabled security domains that govern each cloud layer to be accurately mapped to security parameters as described in the evaluation framework. In the chapter, the evaluation of security provisions offered by the CSP on both cloud models were evaluated against a set of customer security requirements gathered from the scenarios. This enabled a proper audit check to determine whether the provisions meet the requirement specifications by comparing both provisions and requirements based on the data set generated from the mapping matrix.

Results from the security assessment test exposed vulnerabilities within the cloud layers which can be linked to vulnerabilities and security mechanisms implemented in each layer of the cloud architectures. The results presented from the assessment highlights vulnerabilities which are linked to security domains in each layer of the cloud models. The analysis of the results gathered from the evaluation and audit checks on both cloud models is presented in the next chapter.

Chapter 8 : ANALYSIS OF RESULTS AND FINDINGS

8.1 INTRODUCTION

This chapter presents analysis of the results and findings from the security evaluation of each scenario and PaaS cloud models considered. Security audit, test and vulnerabilities assessments conducted in both scenarios are analysed in detail.

8.2 ANALYSIS

The security assessment tests highlighted vulnerabilities within the PaaS cloud architectures which can be linked to specific security requirement domains and cloud layers. Results also indicate cloud layers where such vulnerabilities can be found which could be linked to management responsibilities, security mechanisms and controls used to secure the respective cloud layers. Although Windows Azure and Windows Azure Pack have similar architectures, the evaluation showed components within the cloud architectures differ as well as security implementations. The security audit check enabled comparison between customer security requirements and security provision implementations. It enabled proper assessment of each security domain and security controls implemented in each one. The security framework demonstrates its effectiveness in the proper evaluation of cloud requirements and provisions which enabled an assessment test and is linked to each layer and security domain of the cloud models. A detailed result and findings analysis of each scenario describing the security audit checks and security assessments are discussed:

SCENARIO 1-SECURITY AUDIT CHECK ANALYSIS

From the security classification and analysis shown in the bar charts (Figure 8.1), Windows Azure offers security provisons that are able to meet the customer's security requirements specifications.

In the Front End, Middle-Tier and Back End Layers, the sum of the security mechanisms provisions on each layer were **7,11, 9** respectively while the sum security requirements in each layer were **7,10 and 9** respectively (Figure 8.1).

The critical areas of focus as highlighted in both barcharts indicated the Middle-Tier layers for both security requirements and provisions. However the security provisions had a higher sum compared with the requirements specifications i.e 11 > 10. Findings from the security classification of security mechanisms in the layer highlighted security capabilities are offered by the security provisions and implementations in Windows Azure. This enhanced security capapbility is managed by the CSP.

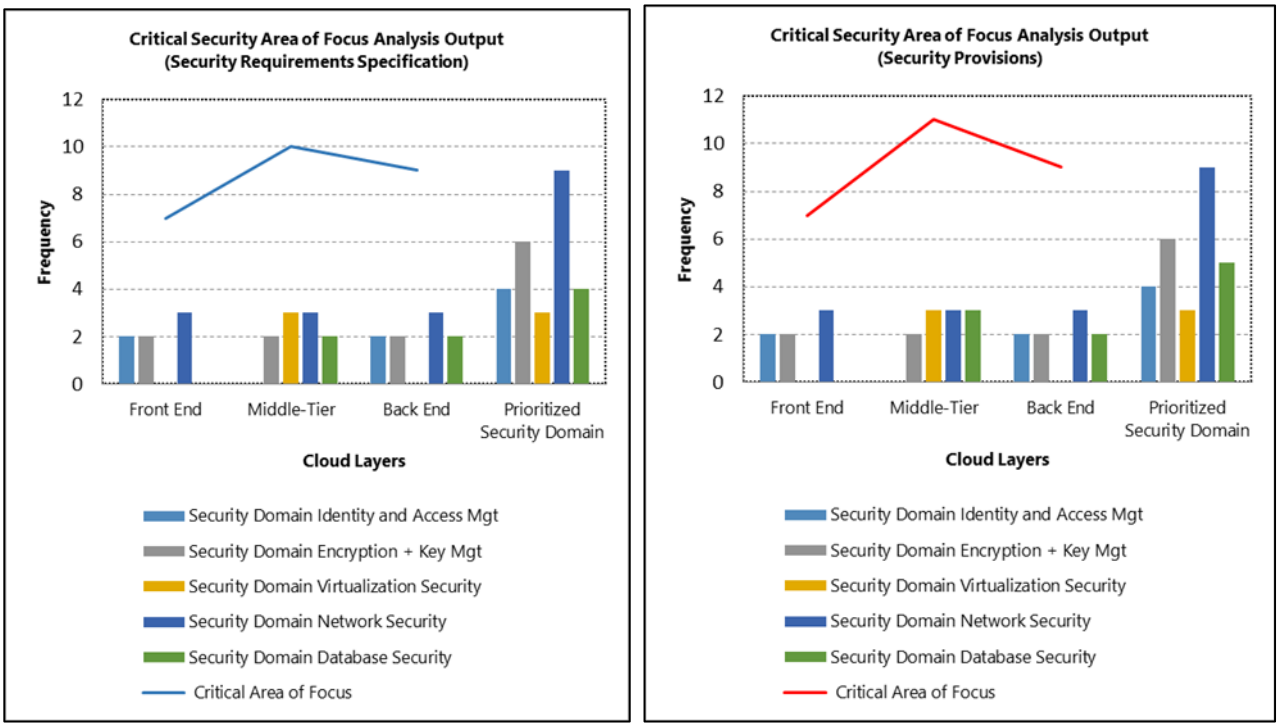

FIGURE 8.1: SCENARIO 1- SECURITY AUDIT CHECK

The enhanced security capabilites is found to be linked to the Database Security domain where Windows Azure offers a stronger security mechanism enforced through the security controls implemented in the domain. The security provision mechanism description is classified as High (3) compared to the Moderate (2) requirement description gathered from the scenario overview.

Moreover, results and findings from the security assessment indicated the Network Security domain as the prioritised security domain where Windows Azure offers high layered security implementations than any other security domain within the cloud architecture. The security mechanism description across the cloud layers were classified as High (3). Assessment showed that this result was due to enhanced security implementations across all communication channels and endpoints between components of the cloud architecture.

SCENARIO 1- SECURITY ASSESSMENT TEST ANALYSIS

Results from the security assessment test highlighted a number of perceived vulnerabilities in each layer of Windows Azure. Perceived security vulnerabilities were found to be relative within Identity and Access Management, Virtulization Security, Network Security and Database Security domains.

However, vulnerability validations were successfully conducted in domains D1 and D3 (Identity and Access Management and Virtualisation Security domains) using the proposed manual techniques described in the research approach and methodology. These validations exposed the Front-End and Middle-Tier layers could be exploited with vulnerabilites in the security implemenations using SSO, WIF and WSUS security controls in the layers respectively.

Having an enhanced security features implemented to strenghten security on these layers will mitigate such threats which will have to be classified and evaluated to ensure they are compliant to meet security requirements and appropriate compliant models. However this will be subject to SLA agreements and additional subscription to the service level required to meet these vunerlabilities.

Perceived security vulnerabilities identified in other layers could not be validated as it would require seeking ethical approval to conduct penetration tests in the Windows Azure cloud environment which at the time of this study could not be initiated.

SCENARIO 2- SECURITY AUDIT CHECK ANALYSIS

From the bar chart graphs shown in Figure 8.2, security audit check highlight the security provisions implemented in Windows Azure Pack did not meet the classified security requirement specifications. The security provision classifications for the Front End, Middle-Tier and Back End layers had the sum of **6, 10 and 8** respectively. However, the requirements specifications sum for each layer were **8, 12 and 11** respectively (Figure 8.2). These results showed that the critical area of focus is the Middle-Tier layer, However the security provisions had a lesser sum compared with the requirements specifications i.e 10 <12.Security provision limitations were found in two domains which are Identity and Access Management and Database Security domains. Security provisions in both domains were classified as Moderate (2). However, security requirements specifications were classified as high.

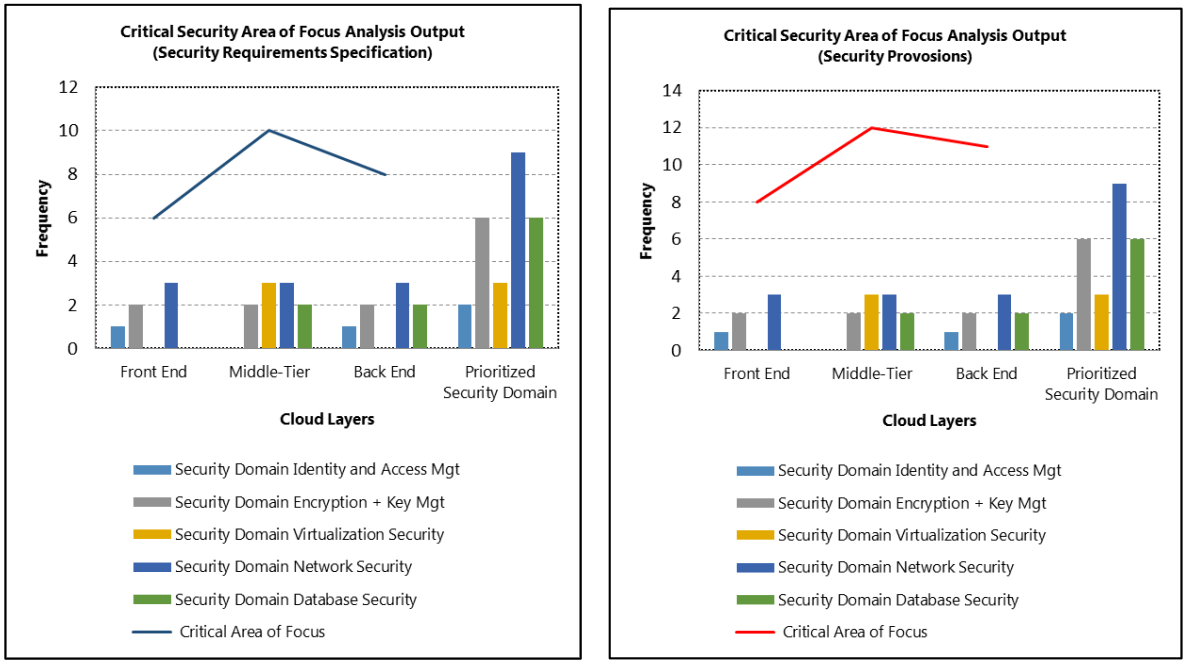

FIGURE 8.2: SCENARIO 2- SECURITY AUDIT CHECK

Moreover, security requirements specification prioritised Network Security and Encrytion/Key Management as domains where enhanced security implementaions will have to be enforced and compliant. Each domain has a classification sum of 9 respectively from the prioritised security requirement specifications. However the findings highlighted security provisions offered, were sufficient for the Network Security domain while Encryption/Key Management had a sum of 6 and did not meet the requirement. This was due to the SSL v2 which was implemented by default in the configuration of Windows Azure Pack. The security control was found to be relativley vulnerable to the security threats which were identified in the security assessment tests.

SCENARIO 2- SECURITY ASSESSMENT TEST ANALYSIS

Security assessment results highlighted a number of vulnerabilities and significant threats in Windows Azure Pack security implementations. Vulnerabilities were found across the three layers within the Identity and Management domain. This results highlights why the sum of classified security

provision in the domain was ranked the lowest from the security audit check and vulnerability validations confirmed the successful exploitation of security threats due to the vulnerabilities identified in all three layers of the cloud.

Successful vulnerability tests were also conducted in security domains which include Virtualisation Security, Database, Encryption and Key Management domains respectively. These findings show that for Windows Azure Pack to meet the specified security requirements in the scenario, additional security features would have to be implemented in each layer of the cloud. The use of the cloud environment would be a risk to a cloud production environment and should be relatively constrained to a test environment only. On the other hand, layers and components in the cloud can be outsourced to a CSP or cloud vendor to provide security capabilities that will enhance security provisions in the cloud.

SECURITY EXCLUSIONS

Security issues that were excluded from the assessment tests were issues that were found to have low or minimal impact based on the simulation proof of concept. Resolution to these security issues and warning were excluded and were found not be have severe impact in the preservation of confidentiality, integrity and availability in the PaaS cloud environment. However in a production environment, these security issues could be considered as minimal or severe risks based on the customer's security requirement specification.

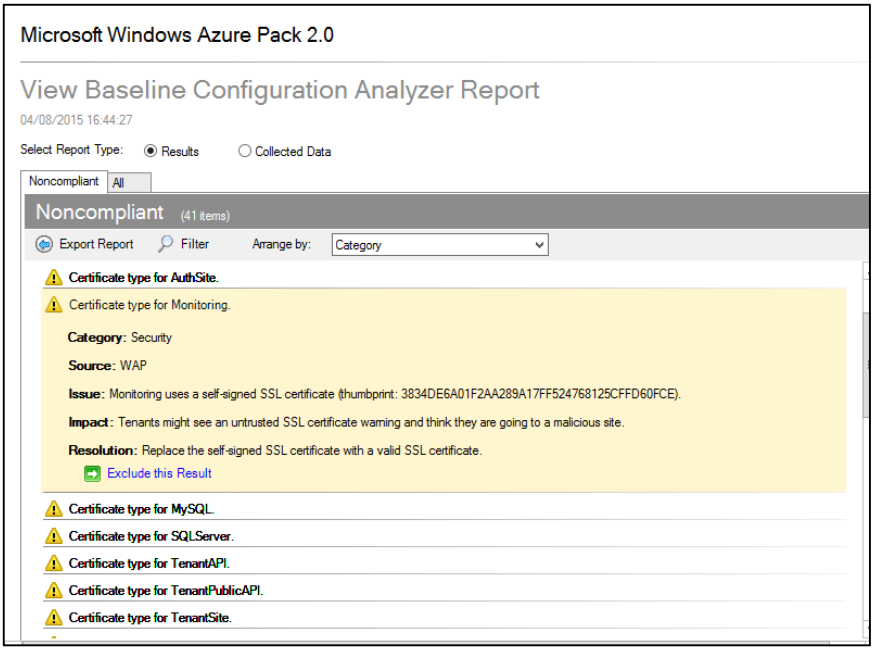

FIGURE 8.3: CERTIFICATE TYPE WARNING

Issue: The warning highlighted in Figure 8.3 above, indicates the authentication site as well as other Windows Azure Pack sites such as the SQL Server, TenantAPI site, AdminAPI site, Tenant site and MySQL site, are using a self-signed SSL certificate within the WAP deployment.

Impact (Low): This however indicates tenants might see an untrusted SSL certificate warning when they try to access the site as they may think they are accessing a malicious site.

Resolution: Replacing the self-signed SSL certificate with a valid SSL certificate issued by a CA.

Action: Result Excluded. No action was taken as the self-signed certificate is valid enough for a test environment as this is a proof of concept environment.

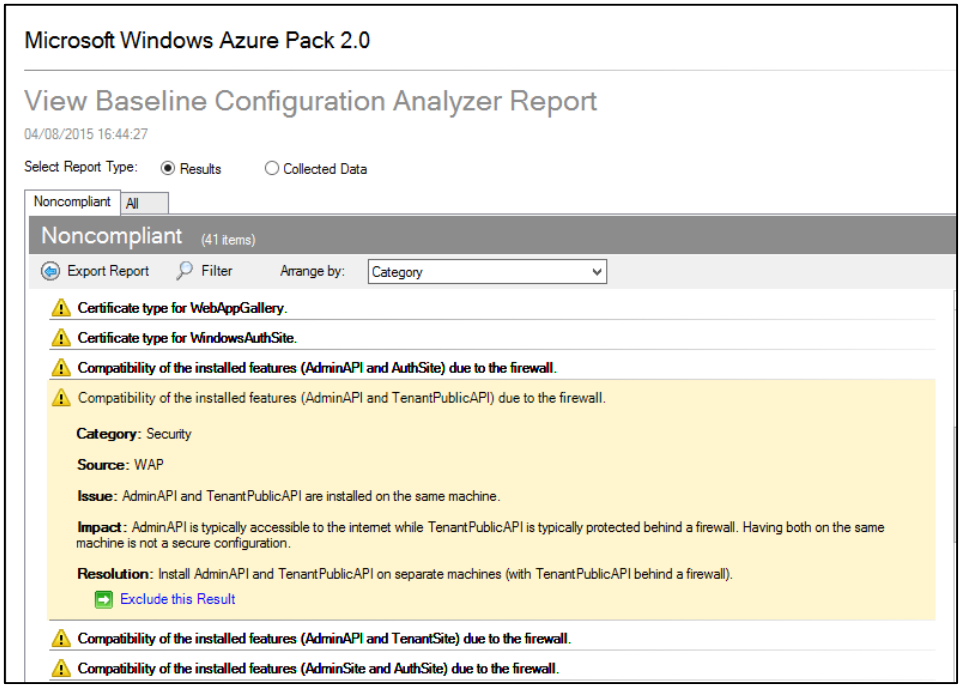

FIGURE 8.4: WARNING SHOWING TENANT PUBLIC API AND ADMIN API INSTALLED ON SAME MACHINE

Issue: The warning highlighted in Figure 8.4 above, indicates the Tenant Public API and Admin API should be configured on separate machines.

Impact (Low): Admin API could be vulnerable to attack since it is on the same domain with the Tenant Public API which is accessible over the internet.

Resolution: Install Tenant Public API and Admin API on separate machines.

Action: Result Excluded. No action was taken as it is a proof of concept within a controlled environment.

8.3 SUMMARY

The analysis of the data generated from the deployment of the security framework and the security assessment of each cloud model based on the scenarios revealed gaps in the security posture of both cloud environments. Security vulnerabilities were based on various issues relative from core technologies used to secure the environment to the nature of cloud environments. The analysis in the chapter discussed the results and findings in detail and offered recommendations that could enhance security provisions to meet the security requirement specifications in both cloud scenarios.

The analysis enabled security issues found within the cloud architectures to be mapped to security layers, components, security domains and stakeholders in the clouds. The deployment of the framework also proved to be effective in order to accomplish the primary aim of evaluating and assessing security implementations in PaaS cloud models.

Chapter 9 : CONCLUSION

9.1 RESEARCH ACHIEVEMENTS

This research highlighted cloud computing security management issues, challenges and responsibilities in PaaS cloud models. The research also discussed current related studies, security frameworks, guidelines and publications that are centred on cloud computing in general with no specific consideration for customer security requirements in the auditing and evaluation of cloud computing deployment and delivery models. The work contained in this thesis is summarised as follows:

This research study was set out to develop a framework that was deployed for security analysis in PaaS cloud models and security architectures. The objectives a critical evaluation of PaaS cloud architectures and its components to develop a reference model which allowed the segregation of the cloud architecture into distinctive layers. This segregation allowed security to be evaluated and assessed using a top to bottom approach on each cloud layer. It allowed PaaS cloud layers and their components to be assessed based on security mechanisms that are used and the multi-layer security architecture that makes the possibility of a malicious attacks difficult.

The developed framework can be adapted to suit customer security requirements from high to medium and basic requirements, in order to enhance security requirements gathering and classification. The framework also enables security analysts to initiate the evaluation and assessment using the processes within the security management cycle. The collated security requirements are mapped using a matrix to identify critical security areas within the cloud architecture were security requirements vary and are represented with quantitative data. The security analysis approach provided a platform for gathering these requirements and comparing them with security provisions

offered in PaaS cloud models. The results and findings enable customers to establish whether a specific PaaS cloud model fits their security needs or has the capabilities to be enhanced through security configurations or SLAs.

The evaluation result highlighted vulnerabilities and threats within the cloud architectures which can be traced to specific layers and security domains in the cloud.

The framework offers more control to cloud customers and enables security analyst to gather specific requirements needed in security evaluations and risk assessment in PaaS clouds. Hence making sure customers get a cloud service model that fits their specific and identified security needs.

Overall, this thesis provided security guidance, security analysis techniques using an adaptive framework and its processes to enable PaaS cloud customers, especially organisations make critical decisions based on security requirements in the adoption and choice of PaaS cloud models.

9.2 RESEARCH LIMITATIONS

The nature, configuration and computer resources used in the simulation of cloud environments made it difficult to consider more than one private or public PaaS cloud model. Having more than one of these to evaluate would have subjected the developed framework to rigorous test of effectiveness in the evaluation and assessment of security provisions of PaaS cloud models. However, the choice of cloud models used is relevant and a leading provider of cloud deployment and delivery model across the I.T industry. The segregation technique also proved useful in the analysis of other cloud vendors which were considered and studied in this thesis.

A typical scenario for a hybrid (Semi-Managed) PaaS cloud model would have been considered in this study. However, this cloud delivery model offers the same services as a private cloud (managed)

with specific services or architectures managed by a cloud service provider. Therefore the evaluation and assessment using the framework will be effective and valid however the management responsibility of certain layers and components will shift from private to public hands.

9.3 RECOMMENDATIONS AND FUTURE WORK

The constant evaluation and review of security features and implementations to ensure they are fit for purpose in PaaS cloud environments requires a methodical approach. Since customer service level objectives and security requirements differ, CSPs must ensure security implementations can be upgraded and downgraded depending on these security requirements to ensure performance and preservation of security.

As cloud service offerings continue to evolve and security attacks become more sophisticated, the developed framework and its processes provides a valuable tool in the evaluation of security implementations to identify critical areas within the cloud architecture and management responsibilities for implementation and configuration of security features to ensure adequate security is guaranteed.

Using quantitative data to represent requirements gathered and security provisions enabled the adequate mapping and matching of security mechanisms to cloud components and architecture layers as well as specific security threats. It allows the auditing process to be specific rather than generic in highlighting critical areas in the cloud where security threats could have severe impact of the customer's data and resources. The adaptive framework also enables security analysts to conduct tests on specific components and highlight vulnerabilities within the cloud architecture with regards to impact on the confidentiality, integrity and availability of computer resources. Organisations can

use the framework to focus on a risk based approach to align security and IT management requirements with PaaS service level objectives. While the framework is intended to evaluate PaaS cloud architectures, it can easily be adapted once security requirements are gathered and mapped into the critical security area of focus matrix to generate output for analysis.

In future, more security evaluations are needed to be carried out on different PaaS cloud architectures based on specific customer requirement scenarios. This will ensure the robustness of the framework which can be adapted to suit the need of other cloud delivery models such as IaaS and SaaS. Further adaptation of the framework is also being considered to ensure the classification of security requirements and provisions can be automated into the mapping matrix to generate output for security analysis.

REFERENCES

[1] D. Sanderson, *Programming Google App Engine*. Sebastopol: O'Reilly, 2009.

[2] Red Hat, "OpenShift," 2015. [Online]. Available: www.openshift.com.

[3] W. Stallings, *Network security essentials: applications and standards*. 2000.

[4] P. Mell and T. Grance, "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology," *Nist Spec. Publ.*, vol. 145, p. 7, 2011.

[5] Information Security Media Group, "Cloud Security Survey," 2012. [Online]. Available: http://www.ismgcorp.com/.

[6] R. Bhadauria, R. Chaki, N. Chaki, and S. Sanyal, "A Survey on Security Issues in Cloud Computing," *Int. J. Innov. Technol. Explor. Eng.*, pp. 83–87, 2011.

[7] T. Mather, S. Kumaraswamy, and S. Latif, *Cloud Security and Privacy*, vol. 1. 2009.

[8] Cloud Security Alliance, "Top Threats to Cloud Computing," *Security*. pp. 1–14, 2010.

[9] M. J. Kavis, *Architecting the Cloud*. Hoboken: Wiley, 2014.

[10] Cloud Standards Customer Council, "Practical Guide to Cloud Computing Version 2.0," 2014.

[11] N. Rozanski and E. Woods, *Software Systems Architecture*. 2005.

[12] A. Alkussayer and W. H. Allen, "A scenario-based framework for the security evaluation of software architecture," *2010 3rd Int. Conf. Comput. Sci. Inf. Technol.*, pp. 687–695, 2010.

[13] M. Armbrust, M. Armbrust, A. Fox, A. Fox, R. Griffith, R. Griffith, A. Joseph, A. Joseph, RH, and RH, "Above the clouds: A Berkeley view of cloud computing," *Univ. California, Berkeley, Tech. Rep. UCB* , pp. 07–013, 2009.

[14] F. B. Shaikh and S. Haider, "Security threats in cloud computing," *Internet Technology and Secured Transactions (ICITST), 2011 International Conference for*. pp. 214–219, 2011.

[15] R. Krutz and R. Dean, *Cloud Security: A Comprehensive Guide to Secure Cloud Computing [Kindle Edition]*. Hoboken: Wiley, 2010.

[16] W. Liu, "Research on cloud computing security problem and strategy," in *2012 2nd International Conference on Consumer Electronics, Communications and Networks, CECNet 2012 - Proceedings*, 2012, pp. 1216–1219.

[17] J. W. Rittinghouse and J. F. Ransome, *Cloud Computing: Implementation, Management, and Security*. 2009.

[18] Fard Systems, "Cloud Computing," *Advanced Products for Today's Businesses*, 2012. [Online]. Available: http://www.fardsystems.com/.

[19] M. Letschin, "The Cloud Explained," 2015. [Online]. Available: www.thesolutionarchitect.net.

[20] K. McDonald, *Above the clouds: managing risk in the world of cloud computing*. GBR:IT Governance, 2010.

[21] I. M. Abbadi, *Cloud Management and Security*. Chichester: Wiley, 2014.

[22] R. Buyya, J. Broberg, and A. Goscinski, *Cloud Computing: Principles and Paradigms*. 2011.

[23] B. Halpert, *Auditing Cloud Computing*. New Jersey: Wiley, 2011.

[24] N. Antonopoulos and L. Gillam, *Cloud Computing: Principles, Systems and Applications*, vol. 54. 2010.

[25] Keith Jeffery Burkhard Neidecker-Lutz, "The future of cloud computing," *Analysis*, vol. 1, no. 1, pp. 1–26, 2010.

[26] R. Bernnat, W. Zink, N. Bieber, and J. Strach, *Standardizing the Cloud - A Call to Action*. 2012.

[27] S. Kumaraswamy, S. Lakshminarayanan, M. R. J. Stein, and Y. Wilson, "Domain 12: Guidance for Identity & Access Management V2. 1," 2010.

[28] CA Technologies, "Security of Cloud Computing Providers Study," 2011.

[29] Ponemon, "Encryption in the Cloud. Sponsored by Thales e-Security," 2012.

[30] Z. Mahmood, *Cloud Computing: Challenges, Limitations and R&D Solutions*. New York: Springer, 2014.

[31] E. Tsyrklevich and V. Tsyrklevich, *Open ID Single Sign On for the internet: A security story*. Las Vegas: Black Hat, 2012.

[32] D. X. Song, D. Wagner, and X. Tian, "Timing Analysis of Keystrokes and Timing Attacks on SSH," in *Proceedings of the 10th conference on USENIX Security Symposium*, 2001, vol. 28913, p. 25.

[33] B. a Sosinsky, *Cloud computing bible*. Indiana: Wiley, 2011.

[34] E. Marks and B. Lazano, *Executive's Guide to Cloud Computing*. Hoboken: John Wiley and Sons, 2010.

[35] V. Eeke, "Presentation by DLA Piper on cloud computing legal aspects," *ISACA*, 2010. .

[36] T. Rodrigues, "What US businesses should know about compliance and regulatory issues before adopting a cloud strategy," *ZDnet-Cloud - How to Do SaaS Right*, 2013. [Online]. Available: http://www.zdnet.com/article/what-us-businesses-should-know-about-compliance-and-regulatory-issues-before-adopting-a-cloud-strategy/.

[37] Microsoft, "Protecting Data in Service Operations," 2014.

[38] Praxiom.com, "ISO 27001 and ISO 27002 Information Security Definitions," *ISO 27001*, 2011. [Online]. Available: http://www.praxiom.com/iso-27001-definitions.htm.

[39] G. Disterer, "ISO/IEC 27000, 27001 and 27002 for Information Security Management.," *J. Inf. Secur.*, vol. 4, pp. 92–100, 2013.

[40] Y. Barlette and V. V. Fomin, "Exploring the suitability of IS security management standards for SMEs," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2008.

[41] Robert R. Moeller, *IT Audit, Control and Security*. Hoboken: Wiley, 2010.

[42] ISACA, "Information Systems Audit and Control Association, ISACA," *2014*. [Online]. Available: www.isaca.org.

[43] Daniele Catteddu and Giles Hogben, "European Union Agency for Network and Information Security: Cloud Computing Risk Assessment," 2009.

[44] U.S Federal CIO Council, "Chief Information Officer Council," 2014. [Online]. Available: www.cio.gov.

[45] M. B. Al Mourad and M. Hussain, "The Impact of Cloud Computing on ITIL Service Strategy Processes," *Int. J. Comput. Commun. Eng.*, vol. 3, no. 5, pp. 367–371, 2014.

[46] M. Rovers, *ISO/IEC 20000:2011 - A Pocket Guide*. Amersfoort: Van Haren Publishing, 2013.

[47] P. Thames, "Can the Cloud, ITIL and ITSM Coexist?," *Leverhawk*, 2014. [Online]. Available: http://leverhawk.com/can-cloud-itil-itsm-coexist-20130925462. [Accessed: 20-Oct-2014].

[48] IBM, "Cloud Computing Use Cases Whitepaper" Version 4.0: Review and summary of cloud service level agreements," 2010.

[49] Cloud Security Alliance, "SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0," *Cloud Security Alliance*, vol. 3. p. 155, 2011.

[50] D. Kelley, "Understanding the CSA Cloud Controls Matrix and CAIQ," *Search Cloud Security*, 2014. [Online]. Available: http://searchcloudsecurity.techtarget.com/feature/Understanding-the-CSA-Cloud-Controls-Matrix-and-CAIQ. [Accessed: 26-Mar-2015].

[51] L. Wu and R. Buyya, "Service Level Agreement (SLA) in Utility Computing Systems," in *Performance and Dependability in Service Computing: Concepts, Techniques and Research Directions*, 2011, pp. 1–25.

[52] D. C. Verma, "Service level agreements on IP networks," *Proc. IEEE*, vol. 92, no. 9, pp. 1382–1388, 2004.

[53] A. Ec2, "Amazon EC2 Service Level Agreement," *Netw. Oper. Manag. Symp.*, vol. 92, no. 9, pp. 1382–1388, 2013.

[54] S. Saxena, "Ensuring Cloud Security Using Cloud Control Matrix," *Int. J. Inf. Comput. Technol.*, vol. 3, no. 9, pp. 933–938, 2013.

[55] D. Thain and C. Moretti, "Abstractions for cloud computing with condor," *Cloud Comput. Softw. Serv. …*, 2010.

[56] I. Iankoulova and M. Daneva, "Cloud computing security requirements: A systematic review," in *2012 Sixth International Conference on Research Challenges in Information Science (RCIS)*, 2012, pp. 1–7.

[57] D. Aisling, "Cloud computing: Data protection issues." 2012.

[58] V. Casola, R. Massimilano, and A. De Beneditis, "On the Adoption of Security SLAs in the Cloud," in *Accountability and Security in the Cloud:*, M. Felici, Ed. New York: Springer, 2015.

[59] S. K. Das, K. Kant, N. Zhang, M. Raj, and M. Di Francesco, *Handbook on Securing Cyber-Physical Critical Infrastructure*. 2012.

[60] ITIL, "IT Infrastructure Library," 2015. [Online]. Available: http://www.itgovernance.co.uk/.

[61] J. J. Lee and Ron Ben-Natan, *Integrating Service Level Agreements:Optimizing Your OSS for SLA Delivery*. Idianapolis: John Wiley and Sons, 2002.

[62] S. Reiff-Marganiec, *Handbook of Research on Service-Oriented Systems and Non-Functional Properties*. Hershey: Information Science Reference, 2011.

[63] European Commission, "Cloud Service Level Agreement Standardisation Guidelines," Brussels, 2014.

[64] D. Rosado, D. Mellado, E. Fernandez-Medina, and M. Piattini, *Security Engineering for Cloud Computing*. Hershey, 2012.

[65] J. Vacca, *Computer and Information Security Handbook*, 2nd ed. Waltham: Elsevier, 2013.

[66] J. Spillner, S. Illgen, and A. Schill, "Engineering Service Level Agreements: A Constrained-Domain and Transformation Approach," 2012.

[67] S. A. de Chaves, C. B. Westphall, and F. R. Lamin, "SLA Perspective in Security Management for Cloud Computing," in *2010 Sixth International Conference on Networking and Services*, 2010, pp. 212–217.

[68] Outsystems, "PaaS - Powering a New Era of Business IT." 2013.

[69] Virtualisation Special Interest Group and P. S. S. Council, "Information Supplement: PCI DSS Virtualisation Guidelines," 2011.

[70] B. Grobauer, T. Walloschek, and E. Stöcker, "Understanding cloud computing vulnerabilities," *IEEE Secur. Priv.*, vol. 9, no. 2, pp. 50–57, 2011.

[71] A. Belapurkar, A. Chakrabarti, H. Ponnapalli, N. Varadarajan, S. Padmanabhuni, and S. Sundarrajan, *Distributed Systems Security: Issues, Processes and Solutions*. Chichester: John Wiley and Sons, 2009.

[72] Atos, "Risks Analysis Framework for a Cloud Specific Environment," 2011.

[73] Gartner, "Gartner Says Cloud Contracts Need More Transparency to Improve Risk Management," Aug-2013.

[74] D. Firesmith, "Specifying reusable security requirements," *Journal of Object Technology*, vol. 3, no. 1. pp. 61–75, 2004.

[75] Open Security Architecture, "IT Security Requirements," 2015. [Online]. Available: http://www.opensecurityarchitecture.org/cms/definitions/it_security_requirements. [Accessed: 21-Apr-2015].

[76] V. (J. R. . Winkler, *Securing the Cloud*. 2011.

[77] I. M. Abbadi, "A framework for establishing trust in Cloud provenance," *Int. J. Inf. Secur.*, vol. 12, no. 2, pp. 111–128, 2013.

[78] Mcafee, "Virtualisation and Risk: Key Security Considerations for Your Enterprise Architecture," 2015.

[79] N. P. C. Priya, "Security Management in Inter-Cloud," *Int. J. Emerg. Trendsing Trends Techinology Comput. Sci.*, 2012.

[80] H. Takabi, J. B. D. Joshi, and G. J. Ahn, "SecureCloud: Towards a comprehensive security framework for cloud computing environments," in *Proceedings - International Computer Software and Applications Conference*, 2010, pp. 393–398.

[81] C. Wang, Q. Wang, and K. Ren, "Towards secure and effective utilisation over encrypted cloud data," in *Proceedings - International Conference on Distributed Computing Systems*, 2011, pp. 282–286.

[82] M. Nabeel, N. Shang, and E. Bertino, "Privacy Preserving Policy Based Content Sharing in Public Clouds," *IEEE Trans. Knowl. Data Eng.*, pp. 1–1, 2012.

[83] M. T. Sandikkaya and A. E. Harmanci, "Security problems of platform-as-a-Service (PaaS) clouds and practical solutions to the problems," in *Proceedings of the IEEE Symposium on Reliable Distributed Systems*, 2012, pp. 463–468.

[84] H. Tianfield, "Cloud computing architectures," in *Conference Proceedings - IEEE International Conference on Systems, Man and Cybernetics*, 2011, pp. 1394–1399.

[85] OpenStack Foundation, "Open Stack Security Guide." 2014.

[86] A. Kumar and B. Lee, "Secure storage and access of data in cloud computing," *ICT Converg. (ICTC), …*, pp. 336–339, 2012.

[87] L. Yan, C. Rong, and G. Zhao, "Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2009, vol. 5931 LNCS, pp. 167–177.

[88] R. Islam and M. Habiba, "Agent Based Framework for providing Security to data storage in Cloud," *15th Int. Conf. Comput. Inf. Technol.*, pp. 446–451, 2012.

[89] {Department of Defense}, "Trusted computer system evaluation criteria," *{Department of Defense}*, pp. 1–116, 1985.

[90] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Futur. Gener. Comput. Syst.*, vol. 28, no. 3, pp. 583–592, 2012.

[91] B. P. Rimal, E. Choi, and I. Lumb, "A taxonomy and survey of cloud computing systems," in *NCM 2009 - 5th International Joint Conference on INC, IMS, and IDC*, 2009, pp. 44–51.

[92] C. A. Da Silva, A. S. Ferreira, and P. L. De Geus, "A methodology for management of cloud computing using security criteria," in *Proceedings of the 2012 IEEE Latin America Conference on Cloud Computing and Communications, LatinCloud 2012*, 2012, pp. 49–54.

[93] C. Kalloniatis, H. Mouratidis, and S. Islam, "Evaluating cloud deployment scenarios based on security and privacy requirements," *Requir. Eng.*, vol. 18, no. 4, pp. 299–319, 2013.

[94] P. Saripalli and B. Walters, "QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security," *2010 IEEE 3rd Int. Conf. Cloud Comput.*, pp. 280–288, 2010.

[95] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1. pp. 1–11, 2011.

[96] T. Probst, E. Alata, and M. Kaaniche, "An Approach for Security Evaluation and Analysis in Cloud Computing," *Marc-Olivier Kill. Safecomp 2013 FastAbstract, Sep 2013, Toulouse*, 2013.

[97] M. Almorsy, J. Grundy, and A. S. Ibrahim, "TOSSMA: A tenant-oriented SaaS security management architecture," in *Proceedings - 2012 IEEE 5th International Conference on Cloud Computing, CLOUD 2012*, 2012, pp. 981–988.

[98] S. Zardari and R. Bahsoon, "Cloud Adoption: A Goal-oriented Requirements Engineering Approach," in *Proceedings of the {2Nd} International Workshop on Software Engineering for Cloud Computing*, 2011, pp. 29–35.

[99] J. W. Creswell, "Creswell, J.W. (2003). Chapter One, 'A Framework for Design.,'" in *Research design Qualitative quantitative and mixed methods approaches*, 2003, pp. 3–26.

[100] M. Bishop, *Computer Security: Art and Science*. Boston: Pearson Education, 2013.

[101] J. Chaula, L. Yngström, and S. Kowalski, "Security metrics and evaluation of information systems security," *Retrieved April*, 2004.

[102] International Systems Security Engineering Association (ISSEA), "Systems Security Engineering Capability Maturity Model," 2008.

[103] Tenable Network Security, "Nessus Vulnerability Scanner." Tenable Network Security, 2015.

[104] K. Scarfone, M. Souppaya, A. Cody, and A. Orebaugh, "NIST- Technical Guide to Information Security Testing and Assessment," 2008.

[105] Google, "Google Cloud Platform," 2015. .

[106] B. C. Kaufman and R. Venkatapathy, "Windows Azure ™ Security Overview," *Security*, p. 58, 2010.

[107] Google, "Google App Engine," *Development*, vol. 2009, pp. 1–10, 2011.

[108] B. Kleyman, "Understanding Cloud APIs, and Why They Matter » Data Center Knowledge," 2012.

[109] R. P. Padhy, M. R. Patra, and S. C. Satapathy, "Windows Azure PaaS Cloud: An overview," *Int. J. Comput. Appl.*, vol. 1, no. 2, pp. 109–123, 2012.

[110] J. Shenk, “Layered Security: Why It Works,” 2013.

[111] G. Rapkin, “Holistic security: taking a multi-layered approach,” *British Computer Society*, 2015. [Online]. Available: http://www.bcs.org/content/conWebDoc/22496.

[112] S. Türpe, “What is the shape of your security policy? Security as a classification problem,” in *Proceedings New Security Paradigms Workshop*, 2009, pp. 23–36.

[113] Defense Information Systems Agency (DISA), “DEPARTMENT OF DEFENSE (DoD) CLOUD COMPUTING SECURITY REQUIREMENTS GUIDE (SRG),” 2015.

[114] National Institute of Standards and Technology, “Standards for Security Categorization of Federal Information and Information Systems,” 2004.

[115] L. Miller, *Network Security in Virtualised Datacenters for Dummies*. Hoboken: John Wiley and Sons, 2012.

[116] Symantec, “5 Essential Steps for Implementing Strong Authentication in the Enterprise 1 |,” Mountain View, 2009.

[117] R. Jennings, *Cloud Computing with the Windows Azure Platform*. 2009.

[118] Microsoft, “What is Microsoft Azure?,” 2015. [Online]. Available: http://azure.microsoft.com/en-gb/overview/what-is-azure/.

[119] B. P. Peddigar and G. Phadke, “Windows Azure – The Cloud Computing Platform,” 2011.

[120] C. Kaufman and J. Sloss, “Windows Azure Security: Technical Insights,” 2014.

[121] L. Lamport, “Password authentication with insecure communication,” *Communications of the ACM*, vol. 24, no. 11. pp. 770–772, 1981.

[122] Barracuda, “Barracuda Web Application Firewalls,” 2015. [Online]. Available: https://www.barracuda.com/support/documentation.

[123] D. Chornyi, J. Reidiger, and T. Wolfenstetter, “Into The Cloud: An Evalution of Google App Engine,” 2010.

APPENDICES

The appendices section consists of additional resources and information that contribute to the research study. They are collated and organised as follows:

Appendix A- PaaS Cloud Architectures

Appendix B- Windows Azure Pack Simulation

Appendix C- Nessus Vulnerability Assessment Scan- Windows Azure Pack

APPENDIX A- PAAS CLOUD ARCHITECTURES

1. Google App Engine (GAE)

Google App Engine (GAE) is a PaaS cloud serviced by Google. It offers customers the capabilities and tools needed to develop, deploy and host applications using resources provisioned by Google on a pay as you go basis. It is categorised as a Managed PaaS cloud.

Similar to other PaaS clouds considered in our study, the Google App Engine architecture is very similar and closely related in the way it functions. Its components can also be segregated into the three distinct layers, Front End, Middle-Tier and Back End.

Layer 1- Front End Layer:

- **Service /Web Management Portal** -This layer ensures customer requests get off the internet and onto the Google network to be handled by the GAE. The dedicated Front Ends take customer data via HTTPS requests and send them across to the Middle-Tier layer to be processed and executed by the Runtime Environment. To manage the Front End, GAE provides customers or users with a console known as the Google Developer Console and Administrator Console. IT allows customers to manage cloud platform resources using their subscription account credentials to access the console portal.

Layer 2- Middle-Tier:

- **Runtime Engine + SDK**- this layer presents itself with an environment where application is executed and deployed onto application hosting servers [123]. The execution and handling of application source codes are invoked by requests sent through communication endpoint channels from the Front End. The Runtime Environment creates instances which is isolated to

an individual user within the multi-tenant cloud environment. Once application requests are handled, responses are sent back through the GAE request handlers using HTTPS communication channels or APIs. Coupled with the Runtime Environment are the tools needed to build web based applications. These tools known as the Software Development Kit (SDK) contains resources and APIs that is used to develop applications which are hosted on Google's cloud platform. The SDK enables applications to be managed on the user's local computer before being deployed via communication channels and endpoints to the runtime environment for execution.

- **Application Containers +DBMS**- Web applications developed and deployed on GAE are hosted on application servers. These applications are supported by database management services where data images, files and objects can be stored. The DBMS offer storage services for customer web applications hosted on dedicated servers include, Google Cloud SQL (Google Cloud SQL is a MySQL database that lives in Google's cloud), Data Store and Memcache (allows storage of commonly accessed data).
- **Abstraction and Operating System**- Individual runtime engines are isolated with runtime environment instances that support different programming languages. Therefore the Abstraction on GAE is supported by virtual instances of runtime environments called sandboxes. The respective sandboxes host languages supported by GAE. Languages supported are Python, Java. PHP and Go.

Layer 3- Back End:

- **Platform Physical Resources + DBMS**- GAE is supported and hosted by Google's Platform physical servers hosted in datacentres. Supported by cutting edge technologies for managing datasets and creating instances for which application can be built and data stored in the

cloud. Database Management Systems (DBMS) on GAE and managed and powered by infrastructures such as Map Reduce, Dremel and Bigtable. They ensure data can be provisioned, stored, queried and retrieved for numerous number of virtual instances running runtime engines and environments.

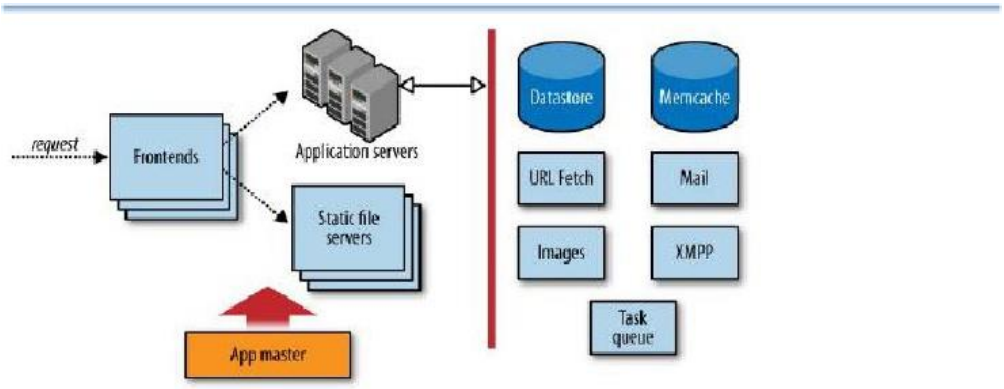

FIGURE A.1: STRUCTURE OF GOOGLE APP ENGINE [1]

2. OpenShift Origin

OpenShift is a PaaS cloud built around a core of application containers and Linux infrastructure to provide developers with a platform to build and deploy web based applications. Over the years OpenShift has developed and many versions of the PaaS cloud have been released. Its recent version OpenShift v3, is a layered system designed to expose underlying Docker and Kubernetes concepts as accurate as possible to provide developers with an application building platform [2].

Similar to most PaaS Cloud architectures, OpenShift v3 provides an architecture overview that highlights its architecture surrounded by service provision through network, compute and storage. In figure 11.2, the core of the cloud architecture runs on Red Hat's Enterprise Linux OS and network nodes that provide communication channels and endpoints to the storage, services and users.

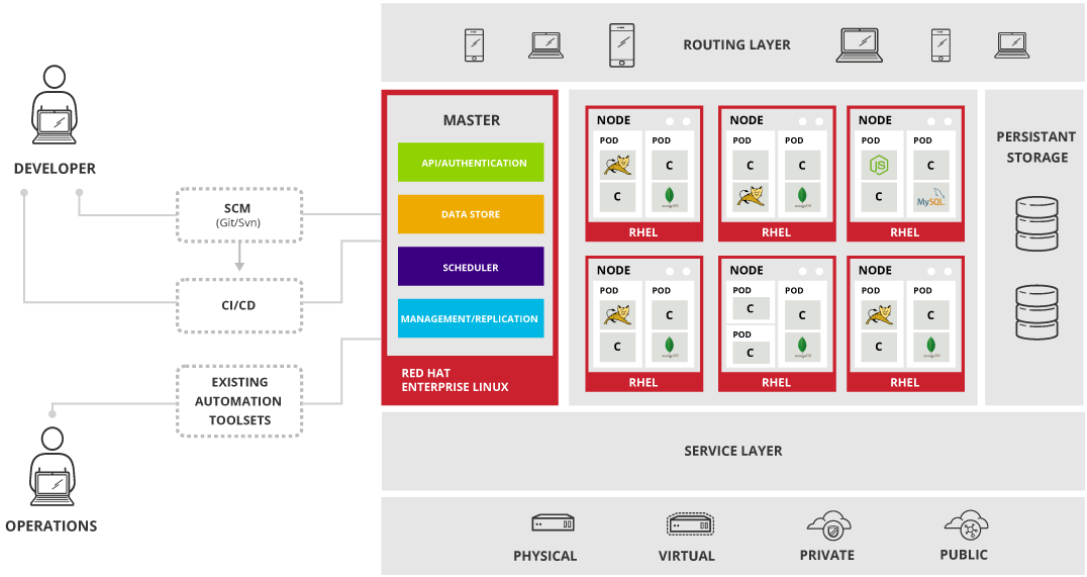

FIGURE A.2 OPENSHIFT ARCHITECTURE OVERVIEW [2]

Layer 1- Front End

- **Service/ Web Management Portal-** OpenShift web console serves as the service and management portal were developers and administrators can manage the PaaS cloud resources. It can be assessable through a web browser which sends initial API requests to cluster servers (containers) running in the Middle-Tier layer.

Layer 2- Middle Tier

- **Runtime Engine + SDK**- The runtime engine on OpenShift are made up of a collection of containers that build application source codes into images. The SDK also known as OpenShift Client tools (rhc) are built and packaged using Ruby.
- **Application Containers + DBMS**- Application containers on OpenShift a represented by Linux containers managed by Kubernetes. Kubernetes, an open source platform powered by Google, automates deployments and scaling of application containers virtually, creates hosts for developed applications in OpenShift PaaS cloud. Linux containers are similar to VMs as

they have core allocations of CPU shares, Bandwidth, Memory and Input/output block. The DBMS for applications are provisioned by data store cartridges created within the cluster of Kubernetes managed containers. They include MongoDB, MySQL and PostgreSQL serve database images for developed applications.

- **Abstraction + Operating System**- Abstraction on OpenShift is provisioned by a Type 2 Hypervisor called Docker. Written in Go programming language the software that runs on top of Linux OS, it provides automated level virtualisation for the deployment of web based application into application containers. Control groups within the Linux OS kernel enables sandboxing and isolation of application containers in the multi-tenant cloud architecture.

Layer 3- Backend

- **Physical Platform Resources and DBMS**- The DBMS on OpenShift is provisioned by etcd. Etcd serves are database management system for CoreOS (Linux containers) which allows application data objects to be read and written on.

  OpenShift v3 can be run locally or on a virtual machine running Windows, Mac or Linux. It can also be run on a cluster of servers running Fedora or OSX. It can also be run on AWS or Google Cloud Engine Infrastructures.

APPENDIX B- WINDOWS AZURE SIMULATION

TABLE B.1 SERVER ROLES AND FUNCTIONS: WINDOWS AZURE PACK CLOUD SIMULATION

Server Role	Computer name	Function	IP Address
Domain Controller	DC.cloud.local	Active Directory Federation Server, Certificate Server	192.168.1.1
Virtual Machine Manager (VMM)	VMM.cloud.local	Hypervisor Manager	192.168.1.11
Hypervisor (Hyper V)	HV1.cloud.local	Native Hypervisor; hosts virtual machines.	192.168.1.22
Windows Azure Pack Server	Wap.cloud.local	Hosts the management portal interfaces for both the administrator and tenants.	192.168.1.99
Service provider Foundation Server (SPF)	SPF.cloud.local	Service Provider Foundation; provides an extendable web service that interacts with VMM.	192.168.1.99
Service management SQL Server	SQL01.cloud.local	Provides SQL instance for hosting Windows Azure Pack services and VMM database	192.168.1.11
PaaS Server Farm	Management Server: MServ.cloud.local	Used by Windows Azure Pack to connect the Website clouds infrastructure across a REST endpoint.	192.168.1.44
	Front End Server- FrontServ.cloud.local	Handles Web HTTP requests from the Front end routes them to the Worker role Serves and responds back to the Front End.	192.168.1.79
	Publisher Servers- PServ.cloud.local	Responsible for publishing website and application contents to the File Server	192.168.1.51
	Worker Role Servers- Worker01.cloud.local	Application container used to host websites	192.168.1.10
	File Server- FServ.cloud.local	Serves as host for website contents.	192.168.1.42
	Control Management Server- CServ.cloud.local	Serves as management controller for the entire server farm	192.168.1.41
	Runtime Database Server- WebSQL.cloud .local	Serves as website runtime database and service management API database	192.168.1.11
	Tenant Application Database Server- MySQL.cloud.local	Serves as database server for hosting developed and deployed web applications.	192.168.1.58

APPENDIX C- NESSUS VULNERABILITY ASSESSMENT SCAN- WINDOWS AZURE PACK

Nessus Scan Report

Tue, 01 Sep 2015 13:11:07 GMT

Table Of Contents

Hosts Summary (Executive)

[-] Collapse All

[+] Expand All

192.168.1.1

Summary

Critical	High	Medium	Low	Info	Total
0	0	1	2	16	19

Details

Severity	Plugin	Name

	Id	
Medium (5.0)	12217	DNS Server Cache Snooping Remote Information Disclosure
Low (3.3)	10663	DHCP Server Detection
Low (3.3)	11197	Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)
Info	10028	DNS Server BIND version Directive Remote Version Detection
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	11002	DNS Server Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35371	DNS Server hostname.bind Map Hostname Disclosure
Info	35716	Ethernet Card Manufacturer Detection
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type
Info	72779	DNS Server Version Detection

192.168.1.22

Summary

Critical	High	Medium	Low	Info	Total
1	0	3	0	14	18

Details

Severity	Plugin Id	Name
Critical (10.0)	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611)

		(uncredentialed check)
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (4.3)	65821	SSL RC4 Cipher Suites Supported
Info	10287	Traceroute Information
Info	10736	DCE Services Enumeration
Info	10863	SSL Certificate Information
Info	10940	Windows Terminal Services Enabled
Info	11219	Nessus SYN scanner
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	51891	SSL Session Resume Supported
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	64814	Terminal Services Use SSL/TLS
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

CServ

Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	19	20

Details

Severity	Plugin Id	Name
Medium (5.0)	57608	SMB Signing Required
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date

		Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	11011	Microsoft Windows SMB Service Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
Info	54615	Device Type

FServ

Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	20	21

Details

Severity	Plugin Id	Name
Medium (5.0)	57608	SMB Signing Required
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure

Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	11011	Microsoft Windows SMB Service Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
Info	54615	Device Type
Info	84047	Hyper-V Virtual Machine Detection

FrontServ

Summary

Critical	High	Medium	Low	Info	Total
0	0	5	1	28	34

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate

Medium (5.0)	45411	SSL Certificate with Wrong Hostname
Medium (5.0)	57608	SMB Signing Required
Medium (4.3)	65821	SSL RC4 Cipher Suites Supported
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10863	SSL Certificate Information
Info	11011	Microsoft Windows SMB Service Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	45410	SSL Certificate commonName Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	50845	OpenSSL Detection
Info	51891	SSL Session Resume Supported
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection

Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	84047	Hyper-V Virtual Machine Detection
Info	84502	HSTS Missing From HTTPS Server

MServ

Summary

Critical	High	Medium	Low	Info	Total
2	0	7	1	29	39

Details

Severity	Plugin Id	Name
Critical (10.0)	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)
Critical (10.0)	82828	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	45411	SSL Certificate with Wrong Hostname
Medium (5.0)	57608	SMB Signing Required
Medium (4.3)	65821	SSL RC4 Cipher Suites Supported
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10863	SSL Certificate Information
Info	11011	Microsoft Windows SMB Service Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	43111	HTTP Methods Allowed (per directory)
Info	45410	SSL Certificate commonName Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	51891	SSL Session Resume Supported
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	66334	Patch Report
Info	70544	SSL Cipher Block Chaining Cipher Suites

		Supported
Info	84047	Hyper-V Virtual Machine Detection
Info	84502	HSTS Missing From HTTPS Server

MYSQL

Summary

Critical	High	Medium	Low	Info	Total
0	0	4	0	31	35

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	57608	SMB Signing Required
Medium (4.3)	65821	SSL RC4 Cipher Suites Supported
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10719	MySQL Server Detection
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10863	SSL Certificate Information
Info	10940	Windows Terminal Services Enabled
Info	11011	Microsoft Windows SMB Service Detection
Info	11153	Service Detection (HELP Request)
Info	11219	Nessus SYN scanner
Info	11936	OS Identification

Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	46180	Additional DNS Hostnames
Info	51891	SSL Session Resume Supported
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	64814	Terminal Services Use SSL/TLS
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	84047	Hyper-V Virtual Machine Detection

PubServ

Summary

Critical	High	Medium	Low	Info	Total
0	0	5	1	29	35

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium	45411	SSL Certificate with Wrong Hostname

(5.0)		
Medium (5.0)	57608	SMB Signing Required
Medium (4.3)	65821	SSL RC4 Cipher Suites Supported
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10092	FTP Server Detection
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10863	SSL Certificate Information
Info	11011	Microsoft Windows SMB Service Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	42149	FTP Service AUTH TLS Command Support
Info	45410	SSL Certificate commonName Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	51891	SSL Session Resume Supported
Info	53513	Link-Local Multicast Name Resolution (LLMNR)

		Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	84047	Hyper-V Virtual Machine Detection
Info	84502	HSTS Missing From HTTPS Server

Runtime

Summary

Critical	High	Medium	Low	Info	Total
0	0	6	1	28	35

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	45411	SSL Certificate with Wrong Hostname
Medium (4.3)	65821	SSL RC4 Cipher Suites Supported
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10144	Microsoft SQL Server TCP/IP Listener Detection
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

Info	10287	Traceroute Information
Info	10736	DCE Services Enumeration
Info	10863	SSL Certificate Information
Info	11011	Microsoft Windows SMB Service Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	45410	SSL Certificate commonName Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	51891	SSL Session Resume Supported
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	66334	Patch Report
Info	69482	Microsoft SQL Server STARTTLS Support
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	84047	Hyper-V Virtual Machine Detection

VM02

Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	18	19

Details

Severity	Plugin Id	Name
Medium (5.0)	57608	SMB Signing Required
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10719	MySQL Server Detection
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	11011	Microsoft Windows SMB Service Detection
Info	11153	Service Detection (HELP Request)
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	45590	Common Platform Enumeration (CPE)
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
Info	54615	Device Type
Info	84047	Hyper-V Virtual Machine Detection

WAP

Summary

Critical	High	Medium	Low	Info	Total
0	0	6	0	30	36

Details

Severity	Plugin	Name

	Id	
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	57608	SMB Signing Required
Medium (4.3)	65821	SSL RC4 Cipher Suites Supported
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10863	SSL Certificate Information
Info	11011	Microsoft Windows SMB Service Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	43111	HTTP Methods Allowed (per directory)

Info	43815	NetBIOS Multiple IP Address Enumeration
Info	45590	Common Platform Enumeration (CPE)
Info	46180	Additional DNS Hostnames
Info	50845	OpenSSL Detection
Info	51891	SSL Session Resume Supported
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	66334	Patch Report
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	84502	HSTS Missing From HTTPS Server

outsystems.cloud.local

Summary

Critical	High	Medium	Low	Info	Total
0	0	7	0	40	47

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	11714	Nonexistent Page (404) Physical Path Disclosure
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (4.3)	65821	SSL RC4 Cipher Suites Supported
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Medium	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits

(4.3)		(Logjam)
Info	10107	HTTP Server Type and Version
Info	10144	Microsoft SQL Server TCP/IP Listener Detection
Info	10147	Nessus Server Detection
Info	10394	Microsoft Windows SMB Log In Possible
Info	10736	DCE Services Enumeration
Info	10761	COM+ Internet Services (CIS) Server Detection
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10863	SSL Certificate Information
Info	11002	DNS Server Detection
Info	11011	Microsoft Windows SMB Service Detection
Info	11154	Unknown Service Detection: Banner Retrieval
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	12634	Authenticated Check : OS Name and Installed Package Enumeration
Info	14272	netstat portscanner (SSH)
Info	19506	Nessus Scan Information
Info	20870	LDAP Server Detection
Info	21643	SSL Cipher Suites Supported
Info	22319	MSRPC Service Detection
Info	22964	Service Detection
Info	24242	Microsoft .NET Handlers Enumeration
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	24786	Nessus Windows Scan Not Performed with Admin Privileges
Info	25701	LDAP Crafted Search Request Server Information Disclosure
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
Info	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure

Info	43829	Kerberos Information Disclosure
Info	45590	Common Platform Enumeration (CPE)
Info	46180	Additional DNS Hostnames
Info	50845	OpenSSL Detection
Info	51891	SSL Session Resume Supported
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	58651	Netstat Active Connections
Info	64582	Netstat Connection Information
Info	66334	Patch Report
Info	69482	Microsoft SQL Server STARTTLS Support
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	84502	HSTS Missing From HTTPS Server

worker01

Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	17	18

Details

Severity	Plugin Id	Name
Medium (5.0)	57608	SMB Signing Required
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Info	11011	Microsoft Windows SMB Service Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	45590	Common Platform Enumeration (CPE)
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
Info	54615	Device Type
Info	84047	Hyper-V Virtual Machine Detection